

City of St. Louis
LYDA KREWSON, *MAYOR*



WE STRIVE TOWARD EXCELLENCE
AD EXCELLEUM CONAMUR

DEPARTMENT OF PUBLIC SAFETY
JIMMIE EDWARDS, DIRECTOR

DIVISION OF CORRECTIONS
DALE GLASS, COMMISSIONER

Memorandum

To: Joan Jennings, City Counselor's Office
From: Kim Maloney, Division of Corrections
621-5848 ext. 1059/ maloneyk@stlouis-mo.gov
CC:
Date: March 17, 2020
Re: Contract -Regional Justice Information Service

Joan,

The enclosed contract was reviewed by Deborah Deuster and requested changes have been made. After review by your office, please forward to the Comptroller's Office. Original Contract and all other required information is included herein.

Please contact me if you have any questions.

Thank you,

A handwritten signature in cursive script, appearing to read "Kim Maloney".

City of St. Louis

LYDA KREWSON, *MAYOR*



WE STRIVE TOWARD EXCELLENCE
AD EXCELLEUM CONAMUR

DEPARTMENT OF PUBLIC SAFETY
JIMMIE EDWARDS, DIRECTOR

DIVISION OF CORRECTIONS
DALE GLASS, COMMISSIONER

February 20, 2020

Honorable Darlene Green
Comptroller
City of St. Louis
Room 212, City Hall
St. Louis, MO 63103

Dear Comptroller:

Please find enclosed for your approval an extension of document number 68043 between the City of St. Louis Division of Corrections and REGIS (A/K/A: Regional Justice Information Service Commission).

Ordinance Authority:	70963
Department Number:	633
Fund Number:	1010
Center:	6330000
Account Number:	5659000
Contract Total	\$129,082.40
FY 20 Encumbrance	FY 20 \$64,541.20
Description:	Comprehensive user access to law enforcement and IJMS services.
Duration of Contract:	01/01/2020 – 12/31/2020
Vendor:	REJIS
Address:	4255 West Pine Blvd. St. Louis, MO 63108
Employer ID Number:	43-1065029
MBE/WBE Participation:	No
Insurance/Bonding Requirements:	No

Sincerely,

A handwritten signature in black ink, appearing to read "Dale Glass", with a long horizontal line extending from the end of the signature.

Commissioner, Division of Corrections

City of St. Louis Division of Corrections Master Contract Agreement

This Agreement is entered into by and between the City of St. Louis Division of Corrections (hereinafter "Division") and the REJIS (A/K/A: Regional Justice Information Service Commission), a joint commission of the City and County of St. Louis, Missouri, organized pursuant to Ordinance Number 57056 of the City of St. Louis and Ordinance Number 7631 of St. Louis County, with its principal place of business at 4255 West Pine Boulevard, St. Louis, Missouri 63108 (hereinafter "REJIS").

This Agreement shall codify the scope of services that have been provided to the "Division" by REJIS under separate agreements. The "Division" may add or delete monthly access and communication services that meet technology or operational needs of the "Division" at any time during this agreement.

Article I - Agreement Term

I.1 Term

REJIS services that are currently provided to the "Division" will continue and the term of this Agreement shall end on December 31, 2021. The Agreement may be renewed by the "Division" for a third year if agreed to by both parties upon the termination of this agreement. A request for contract renewal shall be submitted within 180 days prior to the current contract end date. Nothing in this Agreement shall operate contrary to the provision of the Agreement permitting cancellation or termination for cause or failure to appropriate funding.

I.2 Management Control Agreement

The "Division" must comply with Criminal Justice Information System (CJIS) and Missouri Uniform Law Enforcement System (MULES) standards for access to REJIS' suite of law enforcement and associated supporting services (hereinafter "LEWeb"). "Division" and REJIS will execute a Management Control Agreement (see Appendix A) to comply with CJIS and MULES standards regarding access to criminal justice information. Each individual requiring access to LEWeb must complete an Operator IDentification (OID) form. The request for access must be approved by the individual's supervisor. Once approved, "Division" will forward all forms to REJIS who will process them to ensure access to services is initiated. Once the forms are processed, the individual will be notified of their unique REJIS LEWeb UserID.

Article II – Scope and Identification of Services

II.1 General Scope

This Agreement is for the Integrated Jail Management System (IJMS) and the REJIS law enforcement suite (LEWeb) provided by REJIS to the "Division" as described in Appendix B and Appendix C.

II.2 Intellectual Property and Data Rights

As Implied under the REJIS operating charter to support regional government entities, REJIS will retain ownership of the developed software and will make it available to any/all regional government entity (entities) that can utilize this capability. REJIS retains title and all copyrights, trade secrets, and intellectual property rights to the software. The "Division" agrees that the software will not be disclosed, given, sold to, or used by another party without approval of REJIS. The "Division" shall retain the rights to all records and data associated with the "Division" in LEWeb and IJMS systems.

Article III – Pricing and Payment

III.1 Fees

The prices quoted for REJIS law enforcement services and IJMS services are described in Sections III.2 and III.3 shall be billed as noted.

Should additional design changes be requested outside the scope of the Agreement, REJIS will provide the "Division" a quote for the additional costs of the work and an addendum to this Agreement will be prepared and agreed upon before the work is started.

III.2 Annual Subscription Fees

The annual subscription fee of \$68,305.00 for IJMS, shall be billed quarterly (\$17,076.25) each year. The Annual Subscription Fee consists of the use of IJMS, resolution of software problems, periodic general software upgrades, and Help Desk services. Refer to Appendix B for additional details regarding the IJMS features.

The Annual Subscription Fee consists of the use of LEWeb, resolution of software problems, periodic general software upgrades, and Help Desk services. Refer to Appendix C for additional details regarding the IJMS

features. The annual subscription fee of \$42,000.00 for the Justice Center and MSI for LEWeb service shall be billed monthly in 12 equal payments (\$3,500.00). The annual subscription fees for these services is identified in the chart below.

Agency	Annual Subscription Fee For 2019	Billing Frequency
Justice Center & MSI IJMS Subscription See Appendix B for details	\$68,305.00	\$17,076.25/Quarterly
Justice Center & MSI LEWeb Service See Appendix C for details	\$42,000.00	\$3500.00/Monthly

III.3 Monthly Access and Communication Fees

Service	Monthly Fee	#	Annual Fee	Description of Service
Secondary Use fee for Justice Center	\$35.00	1	\$420.00	This secondary use fee is for the connection from Justice Center to REJIS.
VPN Tunnel for Social Security Administration (SSA)	\$60.00	1	\$720.00	This fee is for the connection to the SSA office so they can download data from IJMS on incarcerated individuals.
Unitec Maintenance (Wrist Band Printer)	\$13.00	1	\$156.00	Unitec is a 3 rd party vendor that provides hardware maintenance. The maintenance agreement on printers covers all parts except "user consumable items" such as ink cartridges, maintenance kits, etc.

IJMS Document Imaging	\$12.00	1	\$144.00	This is for storage of inmate fingerprints.
-----------------------	---------	---	----------	---

Annual Fees

Service	Total Fee	Description
Inmate Locator Search Maintenance	\$4,470.40	This is on going maintenance for REJIS to host the Inmate Locator Search.
Media Services (One booking photo capture station)	\$2,000.00	This system is used to capture and store booking photos in a regional database.
St Louis City Jail Population Dashboard	\$10,867.00	Hosting services for inmate population statistics dashboards with 99% service availability.

III.4 Billing

Any bill submitted by REJIS to the "Division" shall have an itemization of the services being billed. Said invoices shall be paid within 30 days of the invoice date. Any late payments shall be assessed a late fee of 1.5 percent for each 30-day period payment is not made.

Article IV – Law and Venue

This Agreement shall be construed and enforced solely in accordance with the laws of the State of Missouri.

Article V – Conflict of Interest

REJIS represents and warrants that no arrangement has been made with any person or agency to solicit or secure this Agreement upon an agreement or understanding for a gratuity, commission, percentage, brokerage, or contingent fee, in any form, to any person excepting bona fide established commercial or sales agency. For breach or violation of this representation and warranty, the City of St. Louis may, by written notice, to REJIS, terminate the right of REJIS to proceed under this Agreement or be entitled (1) to pursue the same remedies against REJIS as it could pursue in the event of a breach of contract, and (2) as a penalty, in addition to any other damages to

which it may be entitled by law, to exemplary damages in the amount as determined by the "Division", which shall be not less than three (3) times nor more than ten (10) times the amount REJIS paid or agreed to pay as such gratuity, commission, percentage, brokerage, or contingent fee. The right and remedies of the City of St. Louis, as provided in this paragraph, shall not be exclusive and are in addition to any other rights and remedies under this Agreement or provided by law.

Article VI - Employees

VI.1 Employee Recruitment Prohibited

REJIS and the "Division" agree that they shall not solicit for employment, nor employ each other's personnel during the term of this Agreement and for six months after termination of the agreement unless a mutual agreement is reached prior to employment commencement. In the event that no prior mutual agreement between REJIS and the "Division" occurs, and REJIS or the "Division" chooses to employ an individual who with the preceding six months was employed by the other party as a full time employee, both REJIS and the "Division" hereby agree to pay an amount equal to six months base salary, without deductions or including benefits to the other party. The base salary will be computed on the employee's salary as of the time of departure from either REJIS or the "Division".

VI.2 Employee Eligibility Verification

REJIS shall execute and submit an affidavit, in a form prescribed by the City of St. Louis, affirming that it does not knowingly employ any person in connection with the contracted services who does not have the legal right or authorization pursuant to Sections 285.525 through 285.55 of the Revised Statutes of Missouri 2000.

VI.3 Living Wage Requirements

Contracts for services in excess of \$50,000.00 may be subject to the City's Living Wage Ordinance (Ordinance #65591). The ordinance requires that, unless specific exemptions apply, all individuals performing work pursuant to a contract between the City and a contractor must be paid a minimum of the applicable wage rates set for the Living Wage Bulletin. If rates are adjusted during the term of the contract, then the applicable wage rates must also be adjusted by the contractor.

VI.4 Non-discrimination

REJIS shall not discriminate against any employee or applicant for employment, or in terms or conditions of employment due to said person's race, religion, creed, color, race, sex, national origin, handicap, or disability relative to carrying out this agreement.

Article VII – Assignment

Except as otherwise provided herein, REJIS shall not, without prior written consent of the "Division" transfer or otherwise dispose of this Agreement, any claim hereunder, any interest herein, or any monies due or to become due hereunder.

Article VIII – Provision of Insurance

REJIS agrees to maintain Comprehensive General Liability Insurance. This coverage shall be on an "occurrence" basis. The minimum limits of coverage shall be one-million dollars (\$1,000,000.00) combined single limit per occurrence for bodily injury and property damage.

Article IX – Severability

The parties agree that should any provision of this Agreement be determined to be void, invalid, unenforceable, or illegal for whatever reason, such provision shall be null and void, but the remaining provisions of the Agreement shall be unaffected thereby and shall continue to be valid and enforceable.

Article X - Confidentiality and Privacy

Both parties acknowledge that REJIS' personnel may gain access to information, the disclosure of which may be restricted by law. REJIS agrees to consider any and all information accessed, received, or discovered in its performance of services under this Agreement as confidential and shall be used only for the purposes of this Agreement, and no such information will otherwise be disclosed by REJIS or its agents or personnel, except as required by law. REJIS and the City acknowledge that the parties may discover each other's proprietary information in connection with the performance of services performed under this Agreement and REJIS and the City agree to receive this information in confidence, to use this information only for the purposes of this agreement, and no such confidential information will be disclosed by the respective parties or their agents without the prior written consent for the other party, except that REJIS and the City may comply with requests for

release of open records in conformity with the provisions of Missouri's Sunshine Law (Chapter 610 RSMo 2000), or other applicable law or order of the court of law with proper jurisdiction. If party receives a subpoena or other validly issued administrative or judicial demand requiring it to disclose the other party's confidential information, such party will provide prompt written notice to the other party of such demand in order to permit the other party to seek a protective order. Each party will be deemed to have met its nondisclosure obligations under this Paragraph as long as it exercises the same level of care to protect the other parties information as it exercises to protect its own confidential information, except to the extent that the application of law or professional standard impose a higher requirement.

Article XI – Warranty

REJIS warrants that the software or services shall substantially perform in accordance with software specifications. REJIS will use its best effort to promptly correct any malfunction. REJIS does not make any other warranties, expressed or implied, nor does REJIS warrant the operation of the software will be uninterrupted or error-free. The City warrants that it will not use the software for any purpose other than as an information-sharing system, and that it will use the software in a manner consistent with the training provided by REJIS.

Article XII – Acknowledgement of Terms and Conditions

The parties hereto affirm each has full knowledge of the terms, covenants, conditions, warranties, and requirements contained in this contract. Each party acknowledges that such party, after negotiation and consultation, has reviewed and revised this contract. As such, the terms of this Contract shall be fairly construed and the usual rule of construction, to the effect that any ambiguities herein should be resolved against the drafting party, shall not be employed in the interpretation of this Contract or any amendments, modifications or exhibits thereto.

IN WITNESS WHEREOF, the parties have executed this Agreement between City of St. Louis "Division" of Corrections and the REJIS Commission dated January 1, 2020.

FOR THE CITY OF ST. LOUIS
COMMISSION

By: _____

Dale Glass
Commissioner

Date

By: _____

Daniel Isom., Ph.D.
Executive Director

Date

02/28/2020

By: _____

Honorable Judge Jimmie Edwards
Director of Public Safety

Date

APPROVED AS TO FORM ONLY:

By: _____

City Counselor

Date

By: _____

Comptroller

Date

By: _____

Register

Date

Appendix A: Management Control Agreement

MANAGEMENT CONTROL AGREEMENT

Between the
City of St. Louis Division of Corrections
And the
**Regional Justice Information Services
Commission**

This Management Control Agreement is made and entered into this ____ day of ____ 2020, by and between the St. Louis Division of Corrections, hereinafter referred to as "Division", and the Regional Justice Information Service Commission hereinafter referred to as "REJIS".

DEFINITIONS

REJIS was established and is governed as a joint commission pursuant to Sections 70.210-70.320 RSMo, as well as Ordinances 57056, 58617, & 64180 of the City of St. Louis and Ordinances 7631, 10598 & 18657 of St. Louis County.

For the purposes of Management Control and applicable security addendums, the "Division" is recognized as a Criminal Justice Agency (CJA) and REJIS is recognized as a Non-Criminal Justice Agency (NCJA) as defined in FBI CJIS Security Policy.

For the purposes of data control, security and protection and this agreement the "Division" requires all criminal justice data provided to or processed by REJIS on behalf of the "Division" to be considered Criminal Justice Information (CJI) as defined by, and thus afforded the protections of FBI CJIS Security Policy, MULES Policy and "Division" policies governing the handling, disclosure and control of the data.

PURPOSE OF AGREEMENT

This agreement provides management control for "Division", which serves as a criminal justice agency authorized under law to receive, process, and store CJI. This management control ensures that any contracted work involving the processing, transmission, storage or sharing of CJI performed by REJIS on behalf of "Division" shall remain under the strict management control of "Division" according to the terms of this agreement and applicable state and federal policies.

Duties of "Division"

Under the terms of this agreement "Division" shall have the authority to set, maintain and enforce the following duties and standards over and/or relating to the access to and control over all CJI and "Division" provided/obtained or owned data and associated processing systems:

- Manage control over, and retain ownership of, any CJI requested by, entered by or received by any employee of "Division" or employee of REJIS who receives criminal justice data on behalf of "Division".
- Access to agency owned criminal justice data and CJIS systems by REJIS
- Policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, applications and other components that comprise and support a telecommunications network and related Criminal Justice and CJIS systems used to process, store, or transmit CJI or any other agency owned data guaranteeing the priority, confidentiality, integrity and availability of service needed by the criminal justice community.
- REJIS' compliance with all applicable federal, state and local laws, FBI CJIS Security Policy, Missouri State Highway Patrol (MSHP) MULES policy and local department policy as they relate to the contracted duties being performed by REJIS on behalf of "Division".
- Monitor the use of CJI records and shall notify REJIS if they are suspending or revoking access authorization and/or lifting any such suspension or revocation.
- Take appropriate disciplinary action upon confirmation of misuse by its employees. Disciplinary actions shall be based upon the agency's policies and procedures.
- Enter records into the REJIS system and be responsible for the content of those records and keep the record content timely, accurate and complete.
- Train their computer terminal operators through training classes that REJIS offers in the use of its services and ensure that training programs are completed and a biennial certification is achieved. (NOTE: This does not replace the MULES/NCIC requirement to obtain MULES/NCIC training and recertify through the MSHP)
- Ensure that all computer hardware/software installed at the [CJA Abbreviation] facility(ies) that are attached to the REJIS/CJIS environment complies with published standards. These standards are available through REJIS.

Duties of REJIS

As a NCJA contracted organization, REJIS may only perform those functions explicitly delegated to REJIS by "Division" in writing as a part of the contract to perform these duties, this agreement or another fully executed

agreement between these two parties. Additionally, REJIS may only provide access to CJIS Systems and criminal justice data under the management control of the "Division" as permitted under this agreement, applicable federal and state law, FBI CJIS Security Policy, MULES policy and any other applicable agreements or contracts executed between both parties of this agreement.

CJIS Connectivity

The type of electronic equipment used by REJIS shall be compatible with the standards set forth in the FBI CJIS Security Policy and shall meet with the approval of the MSHP Information Security Officer (ISO) and the "Division" Local Agency Security Officer (LASO). The use of any CJIS interfaces or connections operated on behalf of "Division" shall be limited to law enforcement/criminal justice purposes and entities with whom "Division" have a current agency agreement on file with the MSHP Security Unit. REJIS must receive written approval before granting any access to the CJIS interface/connection or data operated/maintained on behalf of "Division" to any agency other than "Division" or subunits thereof. All such interfaces or connections must also meet all FBI and MSHP CJIS technical specifications and security safeguards.

Screening of REJIS Personnel and Contractors

All REJIS employees and contractors with either physical or logical access to CJI and/or unescorted access to terminals processing CJI must each sign an FBI CJIS Security Addendum and submit to a fingerprint-based background check pursuant to MSHP CJIS fingerprint policy. Fingerprints must be submitted to either the "Division" or the MSHP CJIS "Division" for inclusion in the Missouri Centralized Vendor File within thirty (30) days of hire. All final determinations for REJIS employee or contractor access to CJI are at the sole discretion of the MSHP CJIS Systems Officer (CSO). Decisions to approve or deny access will be provided to REJIS in writing. However, any denials will only be based upon the reasonableness of the denial action. A list of authorized REJIS employees/contractors will be maintained by "Division" or in the Missouri Centralized Vendor File.

Dissemination

Any REJIS employee or contractor who has access to or receives CJI shall only use the access and data for the purposes for which access was required and it will not be disseminated to any other party without explicit permission from the "Division".

Audit

REJIS computer equipment, facilities, policies and procedures as well as agency-owned data are subject to and shall be made available for Policy Compliance Reviews, Technical Security Audits and routine review by "Division" staff, MSHP CJIS auditors or FBI CJIS auditors. REJIS must allow the aforementioned personnel necessary access to audit, implement and enforce security control as defined by FBI CJIS Security Policy.

Security

REJIS agrees to limit access to CJI owned by "Division" or furnished by MSHP or FBI CJIS in strict accordance with NCIC, Nlets, MULES, FBI CJIS Security and "Division" policies and regulations. REJIS agrees to take full responsibility for the integrity of the CJI stored or processed by REJIS on behalf of "Division". REJIS shall not be held responsible for the misuse of CJI by non- REJIS personnel/contractors. All REJIS personnel or contractors with direct or indirect physical or logical access to CJI shall complete security awareness training pursuant to FBI CJIS Security Policy every two (2) years. REJIS is also responsible for implementing adequate physical security measures at their facilities to protect against any unauthorized personnel gaining access to computer systems, network equipment, storage devices or areas containing/processing CJI. REJIS must provide a complete copy of all "Division" owned data upon written request in a mutually agreeable format within thirty (30) days of request to "Division" to allow for the properly inspection and integrity assurance checks of the data. REJIS shall not provide any CJI commercially or extract any metadata for use by REJIS except within the official scope of duties performed on behalf of "Division". Additionally, all CJI data and backups thereof shall remain the property of and under the control of "Division".

Network Diagram

REJIS is responsible, based on FBI CJIS Security Policy, for providing a network diagram depicting the REJIS network configuration including the location of all computer equipment, connectivity to CJIS and "Division" as well as the data flow within the "Division" network. This network diagram must be updated whenever substantial changes occur or at least every three (3) years and submitted to the MSHP ISO for review and approval.

Misuse

"Division" agrees that any misuse of CJIS systems or CJI obtained by or stored on behalf of "Division" by REJIS or REJIS' personnel or contractors is a Class A Misdemeanor pursuant to 576.050 RSMo as well as a security

incident and as such must be reported to "Division" and to the MSHP CSO and ISO.

Suspension of Service

"Division" reserves the right to suspend all use of CJI owned by, or any CJIS connection operated on behalf of "Division" when any terms of this agreement, or documents incorporated herein are violated by REJIS or REJIS' employees or contractors. Prior to this suspension of connectivity/data use, REJIS shall be notified in writing by "Division" of any alleged violations by "Division" of this agreement. REJIS shall then have five (5) business days to provide a written response to "Division" regarding the notice of violation. If the alleged violation has been satisfactorily resolved use of the data and/or CJIS connections will not be suspended and "Division" shall provide REJIS with written documentation of the fact. If the remediation or planned remediation of documented violations does not meet the terms of this agreement "Division" will notify REJIS of a suspension date in writing. The suspension date will be no less than ten (10) business days from the date "Division" notifies REJIS of the forthcoming suspension. After connectivity and use of the CJI has been suspended, "Division" shall resume furnishing such access and information to REJIS upon receipt of satisfactory proof that such violations did not occur or that such violations have been fully corrected or eliminated. If satisfactory proof is not received by "Division" within thirty (30) days following the suspension this agreement will be considered cancelled for non-compliance and will invoke the cancellation section of this agreement.

Cancellation

"Division" or REJIS may cancel this agreement with or without cause upon thirty (30) day notice in writing to the other party. Upon cancellation any and all data/CJI owned by "Division" shall be furnished to "Division" by REJIS in a mutually agreeable format within (30) days of the receipt of the cancellation notice. Upon notification by "Division" to REJIS that the data has been received in an acceptable format REJIS shall remove and destroy any "Division" owned data from any systems, databases or backups thereof operated by REJIS.

Charges

The ordinances that established REJIS require that REJIS recover its operating expenses through fees for its services. Each criminal justice agency is charged by the amount and type of service it uses. For each calendar year, the REJIS Commission sets a maximum charge for each agency. REJIS invoices these charges monthly, with payment due upon receipt of the invoice.

Incorporation

The following documents and legislation are incorporated into this Management Control Agreement:

- NCIC 2000 Operating Manual and related Technical and Operational Updates (TOUs)
- NCIC 2000 Code Manual
- Interstate Identification Index (III)/National Fingerprint File (NFF) Operational and Technical Manual
- FBI CJIS Security Policy, Version 5.2
- FBI CJIS Security Addendum
- Nlets User and Technical Guide
- MULES Policies and Procedures Manual
- MULES Terminal Agency Coordinator (TAC) Guide
- MULES On-the-Job Training (OJT) Workbook
- MSHP CJIS Purpose Code X Manual
- MSHP CJIS Policy Compliance Review Reference Manual: Fingerprint-Based Identification for Non-Criminal Justice Purposes
- All MSHP CJIS Newsletters
- Minutes of FBI CJIS Advisory Policy Board Meetings
- Bylaws for the FBI CJIS Advisory Policy Board and FBI CJIS Working Groups
- Title 28, CFR, Parts 16;20;25;50;901;906
- Title 5, USC, Chapter 91
- Title 28, USC, Sections 552;552a;534
- Title 42, USC, Chapter 72
- Title 42, USC, Sections 14611-14616
- Public Law 92-544
- RSMo Sections
43.010;43.120;43.401;43.500;43.509;43.515;43.532;43.535;43.543;2
10.482;221.510;301.230;302.225;304.155;304.158;313.220;388.625;45
5.101;455.050;455.085;559.107;571.101;571.104;576.050;577.001;577.0
05;577.023;577.51;589.410;590.010;610.120

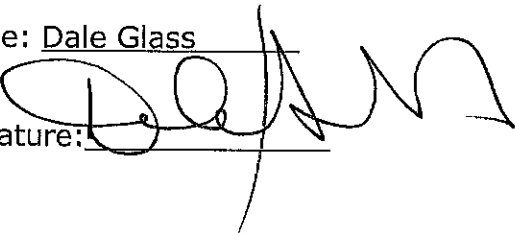
Acknowledgement

WE THE UNDERSIGNED, AGREE TO COMPLY WITH THE DUTIES, RESPONSIBILITIES AND TERMS NAMED IN THIS MANAGEMENT CONTROL AGREEMENT. WE UNDERSTAND THAT FAILURE TO COMPLY WITH THESE DUTIES AND RESPONSIBILITIES MAY RESULT IN SACTIONS BY THE "DIVISION", MISSOURI CJIS SYSTEMS OFFICER AND/OR THE FBI CRIMINAL JUSTICE INFORMATION SERVICES ADVISORY POLICY BOARD, UP TO AND INCLUDING TERMINATION OF ACCESS TO CJIS.

IN WITNESS WHEREOF, the parties hereto have executed this agreement as of the date set forth below.

"Division" Commissioner:

Name: Dale Glass

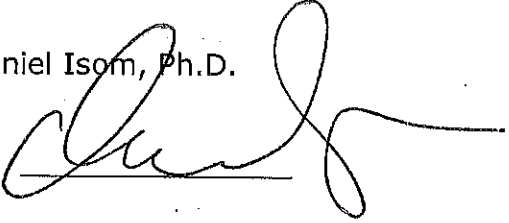
Signature: 

Title: Commissioner

Date: 3-13-20

REJIS Commission:

Name: Daniel Isom, Ph.D.

Signature: 

Title: Executive Director

Date: 2/28/2020

Appendix B: REJIS Jail Management System Software Functions & Features

The REJIS Jail Management System (IJMS) is a fully functional regional solution that encompasses jail operations from initial Inmate Intake Processing to Inmate Release and 15 system interface capabilities. An overview of the primary features of the REJIS IJMS solution follows. The REJIS Solution Set is as follows.

Operational Environment

Facility Infrastructure

The REJIS Hardened Data Center Facility provides all required infrastructure elements to ensure effective and efficient jail operations.

Communications

City of St. Louis Division of Corrections currently has a secure connection into the REJIS network.

Hardware/Software

IJMS functions as a SAAS or ASP model. All required backend hardware and software is included in the annual subscription cost for the service. This includes: redundant servers, server OS, data base software, security software, anti-virus protection, storage, backup software, backup media, off site backup storage, capacity upgrades, and full maintenance support of all hardware and software components. Ongoing annual subscription also includes ongoing upgrades to all server OS, backup, anti-virus, and data base software components.

Aliases

IJMS provides for current booking data, master ("true") data and alias data. The current booking data associates a particular name, social security number, operator license number, state and year, place of birth, and other pedigree information (height, weight, etc.) to a particular booking. The master data contains the "true" name, social security number, date of birth, place of birth, race, sex, other pedigree information, and identification numbers (i.e. State ID (SID), FBI, etc.). The alias data consists of names, nicknames, social security numbers, dates of birth, and operator license numbers. Searches performed in IJMS by name/date of birth/social security number, search booking, true and alias data. The result of a search lists inmates meeting the

search criteria. The booking, master, and alias data for each of the inmates can be viewed without having to perform the search repeatedly. All inserts/updates/deletes are captured and can be searched and viewed from the IJMS Audit module. All objects within IJMS are securable. Objects consist of modules, tabs, screens, fields, reports and buttons. Since the alias data is associated with the inmate master number, attaching a new booking to an existing inmate master number will result in the aliases being carried over to the new booking.

Arrest Circumstances

The IJMS Arrest component records data surrounding the arrest of the offender with many of the data entry elements table driven and configurable by the client from the Administration module. Additional arrests are easily added to a booking allowing for multiple arrests being associated with a single booking. The Arrest data elements include tracking number, arrest number, arrest type (client-configurable), complaint number, arrest date/time, arresting agency (client-configurable), hold for agency (client-configurable), arresting officer DSN, arresting officer name, domestic violence flag, DNA test required indicator, arrest location type (address, intersection, other), address information dependent on arrest location type selected, and arrest notes. Recording of strip search information includes search permitted based upon (client-configurable), date/time of search, location of search, who conducted / observed the search (client-configurable), free-form text for entry of weapons, criminal evidence, other contraband or other condition found, reason for search checkboxes (concealing a weapon, concealing a contraband, concealing criminal evidence, other condition), free-form text for entry of explanation of specific facts causing "reasonable suspicions" that strip search was necessary, and witnessed by agency, officers/persons to the inmate exhibiting violent behavior during or subsequent to arrest.

Boarding of Inmates

IJMS has data entry fields for Billing Agency (client-configurable) and Billing Start Date/Time at the charge level. The IJMS Reports module provides the users the ability to produce Agency Billing Reports. This report is parameter driven allowing the entry/selection of a date range, the facility, a billing agency (or all billing agencies), sort order, and optional heading. The report lists the agency, booking number, inmate name, housing location, booking date/time, released date/time, arrest type, billing start date/time, billing end date/time, and number of days to bill.

Bond Management

Professional bonding companies are maintained in the IJMS Administration module. Relevant data includes company name, name, address, phone number, active/inactive status, inactive date/time and is fully audited. Bond types include Appeal, Cash, Find and Cost, Multi-Bond, Percentage, Personal Obligation, Professional, Property, and Recognizance.

Charges

Charge information consists of charge data in association with an inmate's arrest with many of the data elements table driven and configurable by the client from the Administration module. Data at the charge level includes charge code including modifier, class, offense type (i.e. felony, misdemeanor), statute, description, OCN (Offense Cycle Number - fingerprint card number), fugitive from, charge notes, bond information (including type, amount, paid indicator, bond number, bond company, bond notes), cause number, court date/time, court (client-configurable), room, reason on calendar (client-configurable), disposition codes (client-configurable), disposition date/time, history of previous dispositions, billing agency, billing start date/time, document type (client-configurable), document number, disposition notes, sentence start date/time, sentence end date/time, sentence years/months/days, probation indicator, death indicator, sentence type (concurrent / consecutive), and sentence notes.

Inmate Commissary

REJIS has two installations that interface with the City Corrections commissary vendor. REJIS has found that the commissary functionality is better served by a vendor that specializes in this technology.

Inmate Associations

Any number of associations can be added to an inmate. All associations are carried over to the current booking when an inmate is attached to an existing inmate master number in the booking process. Association types are domestic violence, employment, external, inmate, officer, staff, victim, inmate visitor, and witness. The associations function exists in the Booking, Classify, Operations and Housing modules.

The association type of 'Inmate' is used in designating an inmate who has a conflict with other inmates. When entering an inmate conflict, the association type of 'Inmate' is selected, then a relationship is selected (client-configurable - i.e. co-defendant, enemy, other, relative), next a search for the inmate is performed either by name or code and from the search results the desired

inmate is selected and the inmate master number, name, race, and sex are populated in the detail of the new conflict record. Notes can also be entered from the detail screen and the record saved. Upon save, a reciprocal conflict of the same type and relationship will be added to the inmate selected.

The screen where the associations are viewed, entered, or updated consists of a list of inmates (based on search performed) with photos, the list of the inmate's associations for the inmate selected from the list of inmates and the detail of the association including the association's photo when a particular association is selected from the list of the inmate's associations. Associations can be printed, activated or inactivated from this screen as well.

IJMS provides a warning with the ability to continue a housing assignment or the scheduling of a housing assignment when the housing location contains enemy, co-defendant and/or relative conflicts. The cell assignment scheduling function lists all associations of type 'inmate' on the screen for a quick visual of the inmate's conflicts.

Throughout IJMS the inmate's short and full profile reports are available for viewing and/or printing using accelerator keys. On every screen which references inmates, Ctrl+S results in the short profile (also known as the booking sheet) being displayed and Ctrl+F results in the full profile (also known as the long profile) being displayed both with inmate photo and the option to print.

The short profile or booking sheet consists of inmate name, pedigree, identifying numbers, estimated sentence end date/time, housing location, alerts, address, aliases, employer, wants and warrant checks, arrest and charge, temporary release history and release (if inmate is released) information.

The full or long profile consists of inmate name, pedigree, identifying numbers, estimated sentence end date/time, housing location, alerts, arrest and charge, cell movement history, address, facility property inmate property/valuables, aliases, wants and warrant checks, associations (based on association type and user's security), temporary release history, release (if inmate is released), and notify upon release contact information.

The IJMS Reports module has reports on conflicts which are parameter driven (i.e. can list all or narrow to just co-defendants or just enemies and can list per entire facility or narrow down to a level or a location within a level, can choose from multiple sort orders and enter an optional heading.

Demographics

From the IJMS Booking process, the current booking data associates a particular name, social security number, operator license number, state and year, place of birth, ethnicity, citizenship, local identification numbers, marital status, unemployment indicator, veteran status, homeless indicator, and other pedigree information (height, weight, eye, hair, and complexion) to a particular booking. The master data contains the "true" name, social security number, date of birth, place of birth, race, sex, other pedigree information (height, weight, eye, hair, and complexion), and identification numbers (local identification numbers, SID, and FBI).

IJMS allows attaching a new booking to an existing inmate master number or generating a new inmate master number. Attaching to an existing inmate master number will bring over any demographic data elements from the master to the new booking that was not entered on the new booking. (Even though the race, sex, and date of birth is entered during the booking process and is used in the search (identification) function, it is only used to update the master race, sex, and date of birth when a new inmate master number is generated. The race, sex, and date of birth are only associated to the master data and not to each individual booking.

IJMS demographic data elements (including non-standard data elements) for each inmate's booking record include name, social security number, operator license number, state and year, place of birth, ethnicity, citizenship, local identification numbers, marital status, unemployment indicator, veteran status, homeless indicator, height, weight, eye, hair, and complexion.

IJMS demographic data elements (including non-standard data elements) for the inmate's master record include name, social security number, date of birth, place of birth, race, sex, local identification numbers, SID, FBI, height, weight, eye, hair, and complexion.

Prior bookings and master demographic data (including non-standard data elements) may be modified from the securable Pedigree Maintenance tab in the IJMS Operations module. Authorized users can easily toggle between the booking and master data. All modifications are audited and are viewable from the IJMS Audit module.

Single Fingerprint Solution

IJMS captures and stores inmate fingerprint images as a part of the Admit process. Used to support positive identification of the inmate at time of release. Includes cost of storing digital fingerprint images on secure database servers located at REJIS. Cost of storage is based on the amount of disk space needed to support the City's requirements.

Document Imaging

REJIS has a document imaging system available within IJMS.

Expungements

IJMS allows for the expungements of bookings or the expungements of specific incidents. Both can be performed with a click of a secured button. The security for these buttons is done by the system administrator from the Administration module where the button can be set to enabled, disabled, or invisible for particular security groups and/or users.

The booking expungement process prompts the user to verify the expungement is desired before actually performing the deletions. The expungement of a booking deletes all of the inmate's records for that commitment. Only an audit of the commitment record deletion remains.

The incident expungement process prompts the user to verify the deletion of the entire incident report is desired. The expungement of an incident deletes all records pertaining to the incident including narratives, persons involved, hearing, hearing narratives, and hearing actions. The audit records of the incident report remain (inserts, updates, and deletions).

General

IJMS is built fully on open standards and supports running on Windows server operating systems.

IJMS is built on architecture that allows version/system upgrades that support custom configurations with no additional programming.

IJMS is based on server technology that supports vertical and horizontal scalability, verified to support a potential user community of at least 400 concurrent users.

IJMS is designed to operate with minimal software on the client machines.

IJMS is designed to support Oracle 10G and above databases.

IJMS has the ability to import/export data for use by external systems applications as required.

IJMS has the ability to utilize Messaging Application Programming Interface (MAPI) compliant e-mail systems.

IJMS has the ability to support Extensible Markup Language (XML) transactions with external systems.

IJMS conforms to state submission standards, DOJ Global JXDM, NIEM, NIST, EFTS and facial recognition collection standards.

IJMS is "user friendly" and can be operated with minimal training by employees who have little or no computer experience.

IJMS provides an up-to-date user manual that can be printed or used as an searchable PDF document.

IJMS provides the ability to define user pull down lists within the application.

IJMS provides the user the option of determining whether there is a match based on existing data, provides the ability to produce a comprehensive response displaying all related records. The system provides the ability to retrieve previously confined inmate information using a variety of search criteria such as inmate name (including diminutive first names), biometric data such as fingerprints and other demographic information to avoid duplicate record information.

IJMS allows the attachment/scanning of documents to be saved or printed either on-demand or automatically triggered based on defined criteria.

IJMS allows exact, soundex, and partial name searches.

IJMS allows definition of required fields according to agency standards.

IJMS allows search criteria to be redefined after initial search from the booking process search.

IJMS has the ability to record digital signatures.

IJMS presents search results in linked lists that guide users to details regarding the record found.

IJMS allows for multi facility/jurisdictional application and access.

IJMS provides a single entry with no need to duplicate data entry.

IJMS provides security that has the ability to restrict data entry, retrieval and approval by individual, groups of individuals, agencies, facilities, and machine.

IJMS promotes maximum use of code tables.

IJMS provides the ability to enter narrative/text fields.

IJMS has the ability to provide multiple narrative sheets featuring spell check and formatting capability resembling a full feature word processor and the ability to modify and retain a history of each version of the narratives.

IJMS provides the seamless ability to access multiple systems from a single workstation.

IJMS provides validation on data entry (e.g. logical edits, edit checks for fields, required fields).

IJMS provides the ability to reuse and/or import data from external sources to eliminate redundant data entry.

IJMS provides field level editing.

IJMS has a sophisticated audit trail that includes but not limited to date/time creation, date/time change, user creating or changing, critical information created or changed, and device used to make change (computer name).

IJMS allows control of access to application and data based upon physical location of the end user device and user credentials. Such location is not based upon a static IP address.

IJMS Client software updates will be distributed and processed automatically without the need for an administrator to log on to the individual client workstations. Note: local computer administrative privileges are required for initial software installation.

IJMS supports multiple facilities with full functionality at each facility (e.g., jail, work release center, prison unit.).

The graphical user interface (GUI) of IJMS is logical, easy to use, and is intuitively understandable to personnel and is not a terminal emulation. This also applies to the IJMS Administration module.

The use of functions keys, shortcuts and other functionalities are consistent throughout IJMS.

The IJMS GUI supplies the most current image and demographic data relative to an inmate is displayed on the screen when performing an inmate-specific activity, online and context sensitive help, selection lists and lookup tables the system administrators can establish, maintain, and change at any time without vendor assistance.

IJMS provides a master name index (search types/criteria) that correlates and aggregates information.

The master name index is a central access point for all information in the IJMS application.

The IJMS application provides the client the ability to make data fields invisible from the Security Module Access function of the Administration module.

The IJMS application provides the client the ability to make data fields un-editable (display only) from the Security Application function of the Administration module.

IJMS provides real-time user feedback upon violations of data integrity constraints.

IJMS provides the ability to utilize digitized signatures from different facility locations and assemble documents with those signatures.

IJMS allows import from various sources.

IJMS has data integrity methods such as, but not limited to, the ability to re-associate a booking from one record to another, seal and/or unseal a record or single booking, expunge a record or a single booking, merge two records into one. This functionality is within IJMS and does not require the administrator to alter records at the database level. This functionality is securable, but not limited to system wide administrators.

IJMS provides user-controlled ability to update inmate custody status. Supported status options include: A-Arrestee, I-Inmate and F-Federal

Grievance

From the IJMS Incidents and Grievance module, users can track the grievances by inmate and record the response provided by staff. This module consists of searches and queues for ease of retrieving and processing incident reports, hearings and disciplinary action, and grievances.

The grievance types are setup and maintained in a table with appropriate codes and descriptions (client-configurable – i.e. commissary, mail, medical, property, etc.).

The grievance number is generated with the first two digits equal to the current year and the remaining six digits a sequential number. The grievance date/time defaults to the current date/time with the ability to alter. The status defaults to active with the ability to alter to complete.

When entering a grievance, the inmate's booking number may be entered or a search can be performed to select the correct inmate. One primary grievance type is selected from the list of grievance types with the ability to select up to six additional (secondary) grievance types from a list of the grievance types. Other data elements captured for a grievance include location long description and detail location information, grievance summary information (expandable for ease of entry/reading), routed to information (up to six users may be selected from list of officers) action officer information (date/time, DSN, name, user id), grievance action taken information (expandable for ease of entry/reading), appeal/investigator information (date/time, DSN, name, user id), return date/time, results (client-configurable – i.e. denied, modified, pending, upheld), and grievance appeal response information (expandable for ease of entry/reading).

Entry of additional persons involved is available from the grievance screen. An unlimited number of additional persons involved may be added to a grievance. Printing of the full grievance as well as an inmate print of a formal grievance response form, and a formal inmate grievance appeal response form is available from the grievance screen.

Inmate Personal Property

Property locations are setup and maintained from the IJMS Administration module for property storage locations, sub-locations, and units within the storage locations. Valuable property locations are also setup and maintained from the Administration module.

Main property locations are entered to define the different property rooms and conveyor belts. Sub property locations are then entered for each of the Main property locations with indicators denoting if the next available storage unit number should be automatically generated when the Main/Sub property location is selected when adding inmate property. A Sub property location can be further divided which is useful in handling automatic selection of property bags from conveyor belts alternating between the different iterations to help

in weight distribution. (For example, a conveyor belt may have two sides A and B. When the sub location of Bag is selected, the system will automatically assign the next available bag from A and the next time the sub location of Bag is selected, the system will automatically assign the next available bag from B and so forth.) The last step is to enter the total number of units for each of the locations. This one entry will create all the individual property units. Additional units can be added after this initial creation. IJMS can accommodate over 99,999 separate locations.

Property locations display an occupied/vacant flag and if occupied displays the inmate master number and booking number of the inmate whose property resides in that location.

Inmate property items are setup in the Administration module for ease of selecting property from dropdown lists when receiving property from the inmate. The setup of inmate property items includes a property code, description, status, color, gender (male, female, or both), returnable (yes/no), whether or not the receiving property item should default and whether it should be automatically selected. Other client-configurable property items include inmate property colors, property condition codes, and the 'Property Release to General' codes.

Inmate property is displayed/received/released as well as printing of receipts and labels from the Booking, Operations, Classify and Release modules. All objects within IJMS are securable. Objects consist of modules, tabs, screens, fields, reports and buttons. All inserts, updates, and deletions are audited.

IJMS allows for receiving inmate property into any property location the client system administrator sets up and once the inmate is through the booking process, can modify the property location with the click of a button and supplying the new property location from the Operations or Classify module.

Inmate property can be received from the inmate or released to the inmate or to others as defined. When receiving inmate property items, the description is populated with the ability to alter, the quantity is entered, the color is selected, and optionally the property's condition can be selected, the property location is selected and the next available storage unit number is populated (if auto generate) with the ability to alter, and any notes are entered. When all of the inmate property is released from a property location, that location is flagged as vacant and the inmate master number and booking number is removed from the property location thus making it available for future selection.

IJMS allows inmate property to be returned and received throughout the inmate's incarceration and provides various property searches and reports throughout the application and from the Reports module.

Inmate property can be released to the inmate one piece at a time or all at once. Who the property can be released to is selected at the time the inmate's property is released from a user-defined dropdown list (i.e. inmate, family, police, attorney, etc.). Additionally, inmate associates can be flagged as 'Can Receive Property' causing the association to also appear in the release to dropdown.

Inmate Release

An inmate appears on the Release queue in the IJMS Release module when all charge dispositions for all arrests for the inmate are set to releasable dispositions. The release queue displays the alerts, priority, task status, inmate full name, booking number, tracking number, race, sex, release notes (which are also updateable), and the inmate photo. The Release module always displays the number of inmates on the release queue. A list of the release queue may be printed from the Release module.

The Release module consists of required and optional tasks with required tasks in red text and optional tasks in black text. The release of the inmate cannot be completed until all required tasks have been performed. A print on each task allows the printing of each task's information.

The required charges task is where the charges are approved or the disposition is changed to a non-releasable disposition causing the inmate to be removed from the Release queue.

The required warrants task is where warrants and warrant checks are run and the result is entered. If the inmate is not cleared for release, the release process will not be allowed. A secured button within the warrants task is available for removing the inmate from the release queue if necessary.

The required fingerprint task acquires a digital fingerprint image from the inmate at the time of release for matching to the inmate digital fingerprint image captured during intake.

If the inmate has property (inmate and/or facility property), the property task is required. If no property was received or issued, this task is optional. If the property task is required, a final release of the property can be selected which will release all the inmate property and return all the facility property at one time.

The questions task is an optional task where questionnaires can be filled out for the Final Release Check List and the Release Questionnaire.

If the inmate has associations flagged with 'Notify on Release' then this task will be required. Otherwise, the task will be optional. If the notification task is required, the entry of the contact and final resolution information must be completed.

The journal task lists all of the inmate's journals and additional journals can be added. This task is optional.

The Final Release task is required. The Warrants task must be completed before the Final Release task can be performed. The Final Release task is where the final release type (client-configurable – i.e. administrative release, straight release, released to federal authority, etc.), release to agency [if applicable] (client-configurable), final release date/time (defaults to current date/time with ability to alter), released by, moved by, and notes are entered. The Final Release task displays all the inmate and facility property, all the warrant checks and results, and the inmate's account balance.

Once all the required tasks have been performed, the completion of the release is allowed and the inmate will be removed from the release queue and their confinement end date/time updated, their status set to 'RELS' and all scheduled events, visits, etc. that have not taken place will be closed out.

IJMS has a variety of release reports available. The reports can be specific to individual inmates and include but are not limited to time computation and housing history information. Reports are available for those inmates ready for release but still in custody and those inmates that have been released for a particular day or dates.

Integration/Interface

IJMS will support an XML import and export of data which will allow St. Louis City to share detainee data with corrections, local police, courts and other justice agencies. We have many proven internal and external interfaces to the justice community that can be replicated for St. Louis City. REJIS has interfaces via ODBC, XML, flat file, FTP, web services (Microsoft .NET and Java) and URL.

Privileges

IJMS allows the recording of any loss of privilege as a sanction imposed for a disciplinary infraction, with an effective date, period of sanction, including

suspension of visits, use of canteen/commissary, movement restrictions, etc. and date of reinstatement of privileges.

Inmate Programs

IJMS does provide the capability to track all events and the status of incarcerated persons through scheduled events, inmate status changes, and inmate history and scheduled event reporting.

The inmate's calendar of events displays from the scheduling function and the inmate's calendar of events can be filtered by event type and /or by date range. The client system administrator can setup an unlimited number of user-defined event types for the scheduling types in the Administration module. The parameter-driven Reports module also allows reporting on scheduled or pending events for a particular inmate, housing location, date range, etc.

Record Merge Utility

IJMS provides the ability to merge duplicate records and unmerge records that were joined in error. There are two securable basic functions available in IJMS: Unlink/Link and Unlink.

The Unlink/Link function allows the user to unlink an inmate's booking (confinement) from its existing inmate master number (IMN) and link it to a different IMN.

This function requires the use of the securable 'Search for IMN Number' and the 'Attach to Selected IMN & Close' buttons from the Pedigree Maintenance tab in the Operations Module.

First a search is performed to locate the booking to be unlinked. The booking to be unlinked is selected and the 'Search for IMN Number' button is depressed causing a search window to display with possible matches for linking to a different IMN as well as the details of the booking to be unlinked.

If the desired IMN to link to is not displayed in the master match list, there is an additional search function for producing a new master match list. Once the IMN to be linked to is displayed in the master match list, selecting it will cause all the bookings for that IMN to be listed for further verification that the correct IMN to link to is selected.

The 'Attach to Selected IMN & Close' button will cause the search window to close and the booking to be unlinked from its existing IMN and linked to the selected IMN.

The Unlink function allows you to unlink an inmate's current booking (confinement) from its existing IMN and create a new IMN. This function requires the use of the securable 'Create New IMN Number' button from the Pedigree Maintenance tab in the Operations Module.

A search is performed to locate the booking to be unlinked. The booking to be unlinked is selected and the 'Create New IMN Number' button is depressed causing the booking to be unlinked from its existing IMN and attached to a newly generated IMN number.

The merged and unmerged records are audited. Link and unlink reports can be run from the IJMS Reports module.

Related Persons

IJMS provides the ability to associate persons having various relationships to in-custody inmates.

IJMS allows for an unlimited number of personal/professional contacts through associations attached to the inmate. Association types include Domestic Violence Victim, Employment, External, Officer, Inmate, Staff, Victim, Inmate Visitor, and Witness. The relationships (i.e. friend, spouse, sibling, etc.) for each of the association types are client-configurable. Associations attached to the inmate remain with the inmate and are listed in descending order by booking date/time. Inmate associations can be inactivated and activated. The print of the inmate's Long Profile will only list the active associations. Inmate associations can be viewed from the booking, classification, operations, and housing modules. However, viewing of inmate associations is based on user security. The inmate association will only display for the user if the user's security level is equal to or is greater than the security level of the association type.

The data elements of the inmate association are dependent upon the association type. The data elements for Domestic Violence Victim, Employment, External, Victim, Inmate Visitor, and Witness association types include name, race, sex, date of birth, operator license number, operator license state, phone numbers (home, pager, fax, business, night, other), address, notes, and yes/no flags for 'Can Receive Property', 'Emergency Contact', 'Notify on Release', 'No Contact Order', 'Visit OK', and 'No Admit.' The Employment association type also has company name and a yes/no flag for 'Unemployed.'

The data elements for both the 'Officer' and 'Staff' associations are personnel id, name, race, sex, phone (home, business, night), notes, and yes/no flags for 'Can Receive Property', 'Emergency Contact', 'Notify on Release', 'No Contact Order', and 'No Admit.'

Most of the data elements for the Inmate association type are populated when the inmate association is selected from the inmate search. The data elements populated include inmate master number, name, race, and sex. A notes field is also available for the Inmate association. Relationship types of Enemy, Relative, and Co-defendant are recommended so warnings will be presented when housing moves are performed where the inmate has enemies, relatives and/or co-defendants in the housing location.

The yes/no flags are tied to specific business rules within IJMS. Here are some examples. When the 'Can Receive Property' flag is yes for an inmate's association, that association will appear in the dropdown selection list of those who may receive released inmate personal property. When the 'Notify on Release' flag is yes on any of the inmate's associations and the inmate is set to be released, the inmate cannot be released without the association(s) being notified of the inmate's release (the Notification task in the Release module becomes required and the contact/resolution must be entered and saved). Only associations with the 'Visit OK' flag set to yes will be available in the selection list of approved visitors when scheduling a social visit. Even though any number of inmate associations can be set to 'Visit OK,' the maximum number of visitors allowed for any one social visit is set at three and an error message will be displayed if an attempt is made to arrive more than three visitors. If the 'No Admit' flag is yes and a social visit is scheduled, a warning will be displayed informing the user the 'No Admit' flag is active at this time and allow the user to continue with scheduling the visit or not. Also, if the 'No Admit' flag is yes, the inmate association will appear on the 'No Admittance Report (Associations)' which can be run at any time from the IJMS Reports module.

Professional contacts (i.e. caseworker, clergy, law enforcement, probation officer, prosecuting attorney, private attorney, public defender, other) can be setup facility wide (not associated to any one inmate) to be used for scheduling professional visits.

Professional contacts can be added/maintained from the Administration module or from the Scheduling module. The data elements for the professional contacts are professional type, name, title, ID, race, sex, firm or company, SSN, yes/no 'No Admit' flag, status (active or inactive), active

date/time, inactive date/time, phone numbers (business, pager, cell), and notes.

If the 'No Admit' flag is yes and a professional visit is scheduled, a warning will be displayed informing the user the 'No Admit' flag is active at this time and allow the user to continue with scheduling the visit or not. Also, if the 'No Admit' flag is yes, the professional contact will appear on the 'No Admittance Report (Professionals)' which can be run at any time from the IJMS Reports module.

Remand

IJMS allows an authorized user to reactivate an inmate's record after they have been released. The reactivation causes the inmate's status to return to active places them on the Housing Transfer List. The user will need to redisposition the charge(s).

The IJMS reactivation has been used for various purposes by our clients (i.e. an inmate is released because another state wants him/her. As inmate is going out the door, falls and is injured and that state refuses to take the inmate because is considered not fit; Inmates are released because another local agency calls and says is coming to pick up six inmates. When bus arrives, only room for four inmates and the extra two inmates must be reactivated; to apply transactions to their account.)

Status Monitor Utility

The IJMS booking and release modules utilize queues to track the order of the inmates received and identify the next inmate required at each process by listing the inmate's key information (full name, race, sex, date of birth, agency specific identifying numbers, housing location, and alerts) and current status. Queues can be sorted by any of the key information items or the current status in ascending or descending order.

The Booking and Release Modules have a tailorable work flow/task list that is table driven. The task lists can be required or optional.

The Booking modules have a Priority Status dropdown selection field which allows the user to select either 24 hour hold or Quick Book & Release. If Quick Book & Release is selected the Priority Release Date/Time field populates to the client's desired number of hours after the Booking Date/Time and rolls the record to the top of the booking queue list with text in red.

IJMS provides for the tracking of an inmate through the booking and release processes at each step of data entry by date and time stamp. IJMS uses

queues to list inmates and show the status of the inmate within the booking and release processes. Various reports and audit provide a precise chronological report of each event and time the event occurred as well as the user performing the event.

System Administration

The IJMS Administration module provides a robust set of administrative functions including application codes, building codes, computers, application security, facility maintenance, scheduling, questions, and reports. This module provides the client with the ability to define and maintain codes and settings particular to their installation.

Application codes are divided into three types – application codes, extended application codes and property application codes and are used throughout the IJMS application for populating dropdown selection lists, setting defaults, providing information and reporting purposes.

Application codes consist of a code, short description, long description, status (active/inactive), entry id, entry date/time, change id, change date/time, inactive date/time, and inactive id. An example of an application code used for a selection list would be Grievance Types (i.e. commissary, education, mail, etc.). An example of an application code used for setting a default would be Idle Timeout with the code containing the number of seconds to allow a user to be logged into IJMS with no activity being performed before suspending IJMS and requiring the user to enter their password to resume use of IJMS.

Extended application codes contain more information beyond the code and descriptions. For example, the Courts application code contains data elements for address, phone, and judge information. Agencies, Disposition Codes, Bond Surety Agents, Inmate Status Codes, Incident Codes, Work Flow Tasks and Housing Unit Profiles are some of the other items configurable from the extended application codes. An example of an extended application code used for setting a default is the Housing Unit Profile which allows the client administrator to assign a housing unit profile to a PC within a housing unit to restrict that PC to a particular housing level or location for cell movement and alteration of inmate status. Officers that need security to move inmates to and from anywhere within the facility can be setup to override housing unit restrictions.

The Property application codes allow the client to define and maintain both inmate and facility property codes and settings.

Inmate property items are setup in the Administration module for ease of selecting property from dropdown lists when receiving property from the inmate. When selecting inmate property items, the description can be overridden and the property's condition can be selected from a user-defined dropdown list. The setup of inmate property items includes a property code, description, status, color, gender (male, female, or both), returnable (yes/no), whether or not the receiving property item should default and whether it should be automatically selected.

Facility property is issued to the inmate or returned to the facility. Facility property items are setup in the Administration module for ease of selecting property from dropdown lists when issuing facility property to the inmate. The setup of facility property items includes a property code, description, status, color, gender (male, female, or both), whether or not the issuing property item should default and whether it should be automatically selected, default quantity, returnable (yes/no), size applicable and sizes.

The Building codes function is used for Facility setup and includes Building, Location, Cell, and Bed setup and maintenance. This function allows the client to define and maintain all the inmate and non-inmate housing locations including visiting booth locations.

The Computers function is used for authorizing PCs for IJMS and defining locations for alert messages (special messaging) for those computers only needing to see alert messages from specific locations. The client security administrator has the ability to restrict IJMS access based on workstation identification.

When a PC is first installed on the network to utilize IJMS an authorization process is necessary. When attempting to run IJMS for the first time the user will receive a message indicating the PC needs to be authorized to use IJMS. The user will need to contact the client system administrator with the computer name in order for the administrator to authorize the PC to use IJMS.

IJMS has a powerful and flexible security system that is administered from the Application Security function. Security authorities and role associations for users are set from the Application Security function.

Users are identified by their login IDs and password. Some institutions use their officers DSN. Passwords are encrypted and must be a minimum of eight (8) characters. All objects within IJMS are securable. Objects consist of modules, tabs, screens, fields, reports and buttons. An administrator creates security user groups. For each of the groups the administrator sets the access

for that security group by disabling, enabling or making visible or invisible the objects. The administrator assigns users to the appropriate security groups. IJMS tracks multiple invalid sign-on attempts and locks a user based on the defined number of attempts. The auditing module indicates who did what when and is viewable by authorized users.

From the Application Security function, the IJMS Reports module is also configurable by the client administrator. The administrator has access to the list of reports available in the system. The administrator associates reports to one or more predefined categories. Categories are associated with user security groups as defined by the administrator.

The Facility Maintenance function is used for defining personnel information including staff qualifications (i.e. weapons qualified, hospital post qualified), shift information and shift qualifications (i.e. qualification and number needed).

The Scheduling function is used to add a watch commander or housing unit shift schedule, add employees to the shift schedule, maintain and print shift schedules.

From the Questions function, client system administrators can define questionnaires to be used throughout the IJMS application.

- Questionnaires can be either single or multiple answer type questions
- Question text as well as text to be displayed next to response (answer) field can be defined
- Questions are defined with the answer as either required or optional
- Questions' visibility within a questionnaire is based on gender (male, female, or both)
- Questions can have the response (answer) type as either yes/no, numeric, text, multiple choice (If multiple choice, must provide each multiple-choice answer text, response type, and any applicable display text)
- Lower and upper limits can be placed on responses (i.e. if question response type is numeric, the lower could be 0 and the upper could be 6, thus only allowing the answers of 0 through 6 inclusive to be valid and any other answers would produce an error message)
- Journals are set to either required or optional and if a Journal is set to required, a two field criteria must be provided along with a label for the journal entry (i.e. if a journal is required and the response type is numeric, the first criteria field would have a dropdown selection of arithmetic operators (>, >=, <, <=, =) to choose from and the second criteria field would be the number to use in the comparison to the

- answer [For example, If criteria is > 3 , an answer of 4 would cause a journal entry screen to pop-up with the label provided]
- An Alert Message type (i.e. Medical, Suicide) can be designated to cause an alert notification to be sent out when a question's answer meets the specified criteria
 - Questions can be divided into sections with section headers
 - Questions can be arranged in the desired order

In addition to print buttons from every function within the Administration module, there is a Reports function for printing such reports as a Cell Report which gives all necessary information building, cell, floor, status, security, male/female, medical, etc. and a Population Summary Report which lists counts of all the buildings, floors, cells by facility.

Inmate Work Detail

The IJMS Work Detail module provides a means to setup unlimited, client-configurable skill sets with an associated hourly value; inmate work detail statuses with each status having a flag for indicating if the status makes the inmate available or unavailable for work detail.

Interfaces

Interface	Exchange Format
Circuit Attorney	FTP flat file
Social Security Administration (additional details in next section)	Flat file generation and Allow access to our web site
Inmate Phone Management System	FTP flat file and web service
Circuit Court	FTP comma delimited file
Appris - VINE - Victim Notification System	ODBC
Commissary Interface	Scheduled Tasks and Web Services
Police – REJIS Arrest Data	IMS file transfer
Sagem Morpho Livescan	Windows service
MULES	Scheduled Tasks
Mug Shot	Real time
Hit Notification	Real time
Wants and Warrants	Real time
State Wide Charge Codes	Real time
Medical Service Interface	Scheduled Tasks
Email notification	Real time

Social Security Administration Interface

A report is generated for inmates confined, convicted / plead guilty, no contest, or serving a sentence. Excluded from the report will be inmates that have been released within 30 days of consecutive admission or those inmates which are classified as Federal prisoners (as identified by the charge which justice services assigns to the inmate).

Division is responsible for their own Internet connection and equipment on their side for connectivity. The connection will be an IPSec connection running AES1, minimum 128 bit encryption. The end points will be a Cisco firewall located at REJIS and a secure device capable of terminating an IPSec tunnel with AES encryption located at SSA. SSA should setup routing so that any connections going to a pre-specified address will be inserted into the VPN tunnel. The only communication from REJIS will be return traffic destined for the host that initiated the connection.

IJMS Reports

Accounting Reports Module

- Account Balancing
- Active Inmate Fund Balances
- Bond transmittal
- Booking Fee Invoice
- Cash Drawer (Moved to Funds Module)
- Check Register
- Fund Activity by Transaction
- Summary of Historical Balances
- Summary of Inmate Accounts

Funds Module

- Bond/Fine Payment
- Cash Bond
- 10 Percent Bond
- Professional Bond
- Property Bond
- Bond/Fines Disbursement
- Check
- Transaction
- Funds Receipts

¹ Short for *Advanced Encryption Standard*, a symmetric 128-bit block data encryption technique.

- Inmate Account Activity
- Cash Drawer Activity

Billing Reports Module

- Agency Billing
- Jail Endorsement Form
- Missouri Tax Jail Time Endorsement

Inmate Lists Module

- Active Inmate Court Listing
- Active Inmate Listing
- Daily Booking Log
- Billable Inmates Report
- Arrest Type of Sentenced Past 45 Days
- Booked Past 90 Days
- Inmates Held for Other Agencies
- List of Inmates Dispositioned Past 5 Days
- Due for Release Listing
- Inmate Facility Counts
- Facility Counts by Sex and Age
- Summary Level Count
- Social Security Administration
- Inmate History List
- Inmate Roster
- Inmate Roster for INS
- Inmates Medical Assessment and Orientation Report
- Inmate Roster for Medical

Inmate Lists Module

- Inmate Roster for Mail Room
- Inmates in Open Seating Roster
- Inmate Roster for Public Defender
- No Court Date Listing
- Satellite Court Release
- Satellite Court Report
- Strip Search
- Summary of Commitments
- Associated Inmates
- Division of Corrections Felonies
- Division of Corrections Inmates
- Incarcerated Veterans Report

- Jail Population Management
- Who Logged In Report
- Inmate Roster for Telephone Technician

Operations Reports

- Veterans Report
- Cautions/Special Conditions Report
- Housing Unit Activity Log
- Incident Report
- Mis Housed Report
- No Admittance Report (Associates)
- No Admittance Report (Professionals)
- Orientation Not Completed within 72 Hours
- Who Resided Where on a Date or Date Range

Scheduling Reports Module

- Court Action Notice
- Court Transportation List
- Charges Report
- Medical Assessment Report
- Scheduled Events Report
- Transportation Trip Ticket

Social Worker Reports Module

- Admission/Release Report
- Pretrial and Sentencing Report
- Appeal Log
- Appeal Log Letter
- Charge Disposition Changed to Sentences
- Disciplinary Hearing Report
- Hearing Log
- Probation and Parole Questions Report
- Probation and Parole Violation Report
- Religious Preferences Report
- Social Worker Sentencing Report
- Statement of Inmate Right

Statistical Reports Module

- Demographics of Floor Report

- Inmates Booked by Arrest Type
- Inmates Released with Disposition of Detainer
- Inmates in Booking Past Four Hours
- Property Verification
- Recapitulation
- Released Inmate
- Summary Booking Report
- Summary Released Report
- Domestic Charge

AD-HOC Reports

- Additional Arrests
- Average Daily Population
- Arrest Entry by Specific Officers
- Misdemeanors and City Ordinance Violations
- Inmates Age 17 October 2006
- Social and Professional Visits April through December
- Admitted to the Justice Center August by Race and Sex
- Bonds for April through December

IJMS Reports

- Total Recognizance Bonds

Appendix C: Law Enforcement Services (LEWeb)

LEWeb is the REJIS Law Enforcement portal that provides access to criminal justice data and client/server based systems in a user friendly, browser-based environment. LEWeb is the primary means for delivering criminal justice applications to the mobile laptop, Smartphones, tablets and desktop environment. Below is the summary of the inquiries and applications available in LEWeb and included in this agreement. Following the summary is a more detailed description of each application along with the valuable interfaces provided.

A. Multi-System Inquiries

REJIS' ability to perform a single inquiry and pull information from a myriad of sources is one of its biggest assets. A single inquiry, known as the Hot File Inquiry, is used to search local, state, and national files.

- Inquiries are automatically sent to MULES, NCIC, Nlets, DOR, State Probation and Parole, and State Corrections with the responses being returned to the inquiring device.
- An individual's photo and information from DOR is retrieved and displayed.
- An inquiry using person information, such as name, social security number, Operator License Number (OLN), or SID numbers, can result in matches from local agencies, DOR, MULES, NCIC, Nlets, State Corrections, and state or federal death certificates. Responses include arrested, wanted, or missing individuals, gang members, parking violators, traffic tickets, driver histories from DOR or Nlets, or individuals that pose a threat to law enforcement or named in field interview reports.
- An inquiry using vehicle information, such as registered owner, license, license tab, or VIN, can prompt responses containing wanted vehicles, parking violations in St. Louis City, stolen vehicles, vehicle registrations from DOR or from other states through Nlets, field interview reports, gang members' vehicles, or vehicles connected to a threat to law enforcement.
- A zip code inquiry can return persons living on a block or street or individuals who are wanted or were arrested based on the severity of the charge (felony, misdemeanor, or local ordinance).
- A CAD Interface is available to allow CAD systems (Global, ITI, Tiburon, etc.) to run inquiries commonly used by dispatchers.
- When an inquiry is made by another agency against a person being tracked in REJIS' Hit Notification System (HNS), the originating agency is

notified of the inquiry and the agency performing the inquiry is made aware of the originating agency's interest in the individual.

B. Arrest/Criminal History

The Arrest system documents the full custody detention of an individual. Information about the arrested individual (name, pedigree, and emergency contact) is collected along with information about the arrest (location, officer, data and time) and the charge(s). Additional information can be added to show bond information, prosecutorial decisions, judicial decisions (including sentence information) and release information. A special feature links arrest records to individuals who were involved in the same event.

A feature monitors the confinement of the individual and sends a notification when the period of lawful detention without a warrant is nearing expiration. An Arrest Watch Summary message is sent at approximately 7am, 3pm, and 11pm to all law enforcement agencies that contains a list of persons arrested during the previous eight hours. On a daily basis a batch report lists all arrests and all releases during the previous 24 hours. An arrest record can be initiated by copying data from the Wanted System or Missing Persons System or from another arrest record for the same individual.

Arrest records are summarized periodically or combined with other arrest events for the same individual to form a criminal history record. If there were insufficient identifiers in the arrest record to associate the arrest event with others, it became a non-summarized record of arrest.

- A Summarized Criminal History record consists of two parts - the "person" information and the "arrest" information. The person information contains the name and alias names along with other identifiers such as ID Numbers (local, county, state and FBI), dates of birth, and social security numbers as well as residence and business address information reported at the time of arrest. The arrest information is a summary of one or more arrests in that jurisdiction for that individual. The arrest information includes the date of arrest, charges, report number, prosecutorial, judicial dispositions and sentencing information when available. Individuals can have multiple records of arrest events/summons, but should only have one criminal history record per agency. Each History record may contain one or more summarized arrest records.
- Criminal History (Non-Summarized Arrests) - If there was insufficient data to associate the arrest record with a criminal history record, the information was moved to the Non-Summarized Arrest file. Non-summarized arrests records are standalone records that were never consolidated. A non-summarized arrest record is an abbreviated version of the full arrest record.
- Record Packing - The process of adding all known additional identifiers to a record to increase the potential that an inquiry will locate the subject of

the record, and minimize any negatives that may develop from stopping someone who shares some of the identifiers with the subject of the record, but is not the subject being sought. To pack a record requires inquiries be made of regional, state, and national systems to determine if there are records there for the same individual that have different identifiers. LEWeb has automated that process through the Record Packing transactions. A second packing transaction will compare the identifiers in a state or national criminal history record with the data entered in the record that is being packed. If the identifier is not in the record being packed it is shown on a listing and made available for selection and automatic addition to the record being packed. An electronic audit trail is created for any identifier so entered. Use of the record packing transactions is a major time saving process to pack records and complies with CJIS standards.

- Validation – Validation is the process of reviewing a record to make certain the information is accurate (no errors), complete (all possible information is included in the record – see record packing), and is current (still active or inactive). Each record is selected for validation according to a schedule established by NCIC/MULES. REJIS has developed a process that automates the process. Select records are reported to the department electronically. An on-line transaction allows the agency to monitor the progress invalidating the records and supports the validation process.

Interfaces Included with the Arrest System

- MULES - Qualified records are automatically sent to MULES.
- OSCA - REJIS could receive a copy of the weekly updates OSCA sends to the Criminal History Repository at MULES. They would be stored at REJIS and displayed with any arrest or criminal history record when the Offense Cycle Number (OCN) and last name match. To initiate the interface between the law enforcement agency and their respective Circuit Courts, authorization must be given to OSCA to forward all future MSHP reporting files to REJIS.
- MEDIA SERVICES - For agencies that use Media Services for capturing booking photos, the Arrest will automatically move textual data to a pending file that is then used to update the Media Services database with minimal operator intervention.
- DWITS - Participating agencies can make use of the DWITS Interface to send arrests with DWI related charges to the state's DWITS system. REJIS worked with the MSHP to automatically capture and forward qualified DWITS charges from the REJIS Arrest system to the MSHP. The DWITS interface eliminates the need for REJIS customers to enter alcohol/drug related arrests into both REJIS and DWITS.
- LiveScan – An image and data from an arrest record can be pulled into the LiveScan document using the REJIS Tracking Number to create a fingerprint card with minimal effort. The "DIVISION" may incur a cost from Sagem Morpho for the service.

- Prosecutors - Arrest records are sent to the St. Louis City and County Prosecutors upon entry into the system.
- Hit Notification System (HNS) - The originating agency is notified when an individual they are tracking is arrested.
- Court System - The St. Louis City Municipal Court uses REJIS' IMDSPlus and upon disposition, the court case findings are extracted from IMDSPlus and added to the corresponding Arrest record.
- Watch Summaries - Public arrests can be made available to attorneys or other entities through our Private Access services.
- Multi-System Inquiry - Matching arrest records can be returned as part of the Multi-System Inquiries available in LEWeb.

C. CrimeMATRIX

CrimeMATRIX is a tool for analyzing crime and locating offenders by identifying relationships among persons of interest across jurisdictional boundaries. LEWeb offers an easy to use web based interface to share with local, state and federal crime data between agencies. The integrated web-based capabilities provide mug shot histories, address histories, arrest histories, Social Security Administration death files, parole and probation information, gun permits, and access to state driver's license records, including photographs. The LYNX analysis software assists the investigator in identifying and locating offenders based on the common data elements of each person and how other associates know one another. CrimeMATRIX searches a number of disparate data bases to assimilate the analysis.

D. Media Services – Mug shots/ Other Images

Media Services replaced the IRIS photo capture system and offers an image capture system that can be used to store mug shots, scars, marks tattoos as well as pedigree and incident data related to the individual. The mug shot of an individual as well as scars, marks, and tattoos are all recorded and retrievable in a searchable format. The system can also be used to create photo lineups and create wristbands for identification during confinement. Line ups are now available with one mug shot per page as well as the traditional 6-pack.

Images can be taken of the face, scars, marks, tattoos, or special or unique items of apparel. The image capture component of Media Services requires the purchase of the necessary hardware and software.

Other images, including crime scene photos, gang, evidence, and/or vehicle photos can also be added in the system. Electronic images

taken with the capture station or imported from other sources can be used to load photos supporting the arrest record. These photos are not required; however, the REJIS arrest record can be used to maintain these photos. Any user with Arrest Update access can add, modify, or remove photos from an arrest record for their agency.

The REJIS arrest database is searched for photo images to use for identification or lineup purposes. Search for photos by:

- Pedigree/SMT – Search for photos on file by name, descriptors and SMT Codes.
- Identifier – Search by LID, CID, SID, FBI and IJMS Inmate Master Number (IMN).
- Arrest – Search by Arrest record identifiers.
- Sex Offender Registration – Search by Registration Type, Zip Code and Offender ID. (This search will be released on a separate date).

Interfaces Included with the Arrest System

- CrimeMATRIX
- The image capture station can be used to capture images for First Responder ID badges.

Media Services Maintenance

REJIS owns all hardware and software used to capture the images. REJIS assesses an annual maintenance fee (\$2,000.00) to offset the costs for making changes and upgrades to the software, hosting the data and maintenance costs on the equipment. REJIS will replace any of the hardware at no additional expense to the department due to use or malfunction.

E. Summons

In law enforcement the referral of an individual to court is documented in the form of an arrest record or summons. The Regional Summons System is used to record non-traffic summons cases. A summons may be issued after a full custody arrest, but is usually reserved for referrals in which a full custody detention did not take place.

Interfaces Included with the Summons System

- IMDSPlus - Upon disposition, court case findings are extracted from IMDSPlus and added to the corresponding Summons record.

- Multi-System Inquiry - Matching summons can be returned as part of the Multi-System Inquiries available in LEWeb.

F. Wanted System

Information about individuals who are wanted (with or without warrants) can be entered in the Wanted System. Information captured includes basic and extended pedigree information and the capability to enter multiple charges. Records can be created for individuals who are wanted for violations of city ordinances, state misdemeanors and felonies, or federal charges. All codes and descriptors in the Wanted System are NCIC compliant. The Arrest System also allows data to be electronically searched to "pack" legacy information into a new wanted person record to save time and reduce the opportunity for error in completing this CJIS mandated task.

Interfaces Included with the Wanted System

- MULES/NCIC - Information entered in the Wanted System is automatically shared with the state (MULES) and national (NCIC) law enforcement systems when the data meets their entry criteria.
- JIS - Both state courts in the St. Louis area extract warrants from JIS and use a web service to send them to REJIS for automatic entry into the Wanted System. The warrants are also be placed in a pending file and await activation by the police department. This provides tighter control over the entry of warrants as the warrant is not moved from the pending file until the police department activates it. Both options require effort on the Court to extract warrant entry/recall requests using a predefined file layout and send them to REJIS. *Note: The interfaces with Circuit Courts will be modified to comply with the agreement between OSCA, REJIS, Automated Law Enforcement Response Team (ALERT), and MSHP as part of the VAWA Grant project.*
- MEDIA SERVICES - A Media Services booking photo can be viewed with the record or printed on the warrant to aid in identification.
- Hit Notification System (HNS) - The originating agency is notified when an individual they are tracking is entered into the system.
- IMDSPPlus - If the St. Louis City Municipal Court uses IMDSPPlus an automated interface between the two systems is used to activate or cancel warrants.
- DOR - An individual's photo can be retrieved from DOR and displayed with the wanted record.
- Multi-System Inquiry - Local wanted records and warrants can be returned as part of the Multi-System Inquiries available in LEWeb.

G. Missing Persons System

Missing person records include full descriptors and data on the person reported missing. All codes and descriptors in Missing Persons are NCIC compliant.

Interfaces Included with the Missing Persons System

- MULES/NCIC - Information entered in the Missing Persons System is automatically shared with the state (MULES) and national (NCIC) law enforcement systems when the data meets their entry criteria.
- Hit Notification System (HNS) - The originating agency is notified when an individual they are tracking is entered into the system.
- Multi-System Inquiry - Missing persons can be returned as part of the Multi-System Inquiries available in LEWeb.

H. Field Interview Reports (FIRS)

Field Interview Report entries are used to document a contact by law enforcement when no arrest is made. FIR entries can be made in a desktop or wireless environment and are purged after two years. It is an investigative aid, providing an account of a location, clothing description, other associates, and vehicle information at the time of contact.

A special feature links FIR records for all individuals who were together at the time of contact. A remarks section allows entry of comments for future reference, such as enforcement action (traffic offenses, trespassing, etc.) that may be of value in future.

Interfaces Included with the FIR System

- Mobile Ticketing - Information entered on a ticket can be used to fill in a FIR entry reducing the keystrokes necessary to complete the entry.
- Multi-System Inquiry - Matching records can be returned as part of the Multi-System Inquiries available in LEWeb.

I. Gang

Gangs, gang members, and vehicles used by gang members can be entered in the Gang Tracking System. Once a gang is identified, information about its name, turf, associate gangs, rival gangs, type of criminal activity, and descriptions of related tattoos or the text of graffiti is entered in the system.

Specific gang members (name, pedigree, ID numbers, scars, marks and tattoos) and vehicles used by the gang members are also added. All gang record entry and re-validation must meet federally recognized standards & protocols.

Interfaces Included with the Gang System

- Multi-System Inquiry - Matching gang members can be returned as part of the Multi-System Inquiries available in LEWeb.
- Hit Notification System (HNS) - Gang members are automatically activated in HNS.

J. Traffic Analysis (Racial Profiling)

The Traffic Analysis system, also known as Racial Profiling, is used to collect the information required by statute and prepare the required reports for the Attorney General. Entries can be made in a desktop or wireless environment.

Interfaces Included with the Traffic Analysis System

- Mobile Ticketing - Information entered on a ticket can be used to fill in an entry reducing the necessary keystrokes.

K. License Plate Recognition (LPR)

REJIS forwards a daily extract of "wanted", missing and outstanding warrant notices to the "DIVISION" for use to detect matches via the License Plate Recognition scan.

Interfaces Included with LPR

- Interface with MULES allows MULES and NCIC data to be included in the daily download.

L. Keep Our Police Safe (KOPS)

Information about individuals and/or vehicles that pose a threat to the safety of law enforcement officers can be entered in this system. The application is designed to allow entry of incomplete information about a situation that may threaten the safety of an officer. An officer can view all threats at any time (i.e., start of shift). In addition, the information is automatically retrieved when an inquiry is made on the subject of the record or the vehicle.

Interfaces Included with the KOPS System

Multi-System Inquiry - Warnings are returned as part of the Multi-System Inquiries available in LEWeb when the person or vehicle information matches.

M. Business File

Emergency contact information for businesses can be entered in the Business File system. The name, address and phone number of business owners and management personnel that can be contacted after regular business hours are entered in this system. An online inquiry by business name or address returns the contact information.

The system can also be used to record emergency contact information for residents as part of special programs such as vacation watches or elderly citizen support.

Interfaces

None

N. Hit Notification System (HNS)

The Hit Notification System (HNS) notifies an agency when another agency contacts or takes some action on an individual of interest to the originating agency.

For example, a probation agency enters the name, race, sex, date of birth and social security number of one of their customers in HNS. They become the "originating" agency. Later, a police agency enters a wanted person record using the same name and social security number. When the wanted record is entered, the application automatically checks the HNS database. Finding a match it sends a "Notification" to the originating agency and to the agency that entered the wanted record that "triggered" the hit. Both agencies are now aware of the interest the other has in the individual. Appropriate follow up action can then be taken.

HNS is included with the LEWeb service at no additional cost.

Interfaces Included with the HNS System

Systems that benefit from being notified when action has been taken on a person being tracked in their system. A number of REJIS Systems utilize HNS to request hits or trigger hits.

Conditions of Probation-Defendants may be handed down additional restrictions to meet probation requirements. If so, the conditions are noted in HNS and displayed when a system triggers a hit on the individual. For example, a subject, Sam, is not allowed to be in the neighborhood park. If he is stopped by an officer who performs a hot file inquiry (multi-system inquiry), a match from HNS would be returned regarding the condition of probation. The officer would be alerted to the restriction and be able to determine whether the subject is in violation at the time of the incident.

O. Message Route

The message route system is used to send and receive free text and formatted messages between criminal justice agencies. Typical use is to request a hit confirmation or to send a hit confirmation or locate notice. Another common use is to send a free text message.

Interfaces

None.

P. Access to State and Federal Computer Systems

REJIS has direct access high-speed communications links with the following state and Federal computer systems using formatted screens.

Missouri Department of Revenue Interface (DOR)

REJIS provides a complete DOR interface from its LEWeb application. The interface provides automated responses from DOR, including DOR photos. LEWeb also allows the following DOR systems to be queried:

- o Vehicle Registration Inquiry (including commercial vehicles)
- o Drivers History Inquiry
- o Marine Registration Inquiry
- o Dealer Registration Inquiry

In addition, REJIS provides batch processing to perform mass retrieval of vehicle registrations at DOR. The process could append vehicle registration information to parking tickets for collection attempts or append prior driver convictions to individuals scheduled for traffic court. The cost for batch processing is not included in the REJIS Services proposal.

MULES/ NCIC Interface

The LEWeb application provides an interface with the MULES system for entry of records into MULES or to pass through to NCIC. The MULES system forwards the data, as appropriate to NCIC and may or may not retain a record in MULES.

The following files are MULES / NCIC only databases:

- MULES Order of Protection
- MULES Stolen Parts
- NCIC ID Theft
- NCIC Unidentified Person
- Vehicle Locate
- License Plate Locate
- Missing Locate
- Wanted Locate
- Order Of Protection
- General Purpose Screen

The National Law Enforcement Telecommunications System (Nlets)

Nlets Inquiries – Inquiries of other databases are supported by Nlets. LEWeb has formats for each of these inquiries so the transaction becomes a fill in the blanks process.

Formatted inquiries are available for:

- Hazardous material (placard) checks
- ORI assignments
- Drug Pointer
- Other states driver history
- Other states vehicle registration
- Generic message format
- Aircraft registration
- Boat registration
- National Insurance Crime Bureau (NICB) files
- Canadian interface for information about people, vehicles, operator license and vehicle registration
- Amber Alert messages

Q. Charge Codes

A charge code is used to specify charges in arrests, wanted, warrants, etc. A charge code is based on a statute and is used to convert to NCIC codes when required. In addition to state felonies, misdemeanors, and infractions, there

are some federal charges and a significant number of local charges. An agency can add their own wording and ordinance number to local charges. The "DIVISION" will use REJIS statewide charge codes.

All REJIS applications involving charges use the Charge Codes. Online inquiries permit the look up of charges and reports list the codes in keyword and numeric order. Charge codes for city ordinance violations can be customized by an agency to include their ordinance number and specific wording.

Interfaces Included with the Charge Code System

- Charge codes are used in a number of REJIS systems including Arrest, Wanted, Summons, Criminal History, *IMDSPlus*, and Mobile Ticketing.

R. LEWeb Interfaces

Several critical interfaces exist in LEWeb to external entities. REJIS understands the necessity to provide continuity of service, eliminate double entry of data, and the efficient exchange of information. Other interfaces will be considered a change request and be addressed in a separate proposal. The following interfaces are included as part of this agreement.

Municipal Courts Interface - The *IMDSPlus* case management system, is fully integrated into REJIS services for case management, warrant processing, DOR conviction notices, attorney, government and private firm access, mobile ticketing, and much more.

- Arrest - Charge dispositions are displayed when the associated arrest record is viewed.
- Summons - Charge dispositions for participating *IMDS* agencies are displayed when the associated arrest record is viewed.
- Warrant - Warrants are activated or cancelled in LEWeb using an automated interface.
- Background Wanted Check - Prior to appearing in court, each individual is checked against the Wanted and Missing Systems to identify those wanted by other agencies.
- DOR - There are two DOR interfaces. When an OLN is entered on a court case, prior convictions are retrieved from DOR and recorded on the case. In addition, conviction information is electronically reported to DOR after the case is dispositioned.
- Mobile Ticketing - Tickets entered in the Mobile Ticketing System are used to create the associated court case record saving data entry time and improving data quality between the entities.

- Red Light Photo Enforcement - After law enforcement validates traffic light violations, they are electronically sent to the court system and the court case is automatically created.
- Court Operational Index - Municipal court information is viewable from LEWeb and to The Missouri Bar.
- Housing Case Load - The St. Louis Housing Department sends a file of cases to be heard in court. The cases are automatically created and docketed.
- Earnings Tax Case Load - The St. Louis Earnings Tax "Division" sends a file of cases to be heard in court. The cases are automatically created and docketed.
- DSN - Police officer name, DSN, and other information is shared electronically with the courts to simplify case assignment and identify officer workload. Other ticket writers, such as health inspectors, can also be entered into system.
- Docket Equalization - The Docketing Equalization System performs officer court scheduling. Computer uses officers' work schedules to assign court appearances on days they are on duty and reduce overtime pay.
- Confined Docket - The police department enters the names of individuals who must appear on the confined docket each morning. When the list is finalized, the associated court cases are created or updated with the court appearance.
- IVR - A robust voice response system is used to save employee time in answering phones.
- POS Registers - Monies collected by the Court are accepted using POS registers. The register information is updated on the corresponding court case. For example, when a case is payable by mail and its payment is entered through the register, the disposition is automatically added to the court case and the case is closed. If payment is made on a warrant case, a warrant cancel is automatically sent to law enforcement.

Circuit Courts (SMC) Interface - Arrests are entered into LEWeb by "DIVISION". REJIS also has an existing interface with the Office of State Court Administrators (OSCA) in which REJIS receives a copy of the weekly updates OSCA sends to the Criminal History Repository at MULES. They are stored at REJIS and displayed with any arrest or criminal history record when the OCN and last name match. To initiate this interface, authorization must be given to "DIVISION" from OSCA to forward all future MSHP reporting files to REJIS.

Additionally, REJIS provides a warrant interface between an agency using JIS and its corresponding police department. There is no requirement to utilize the interface, but it does expedite the entry of warrants into the Wanted System. There are two options available.

1. The warrants can be placed in a "pending file" which is used by the police department to move records into the Wanted System through an activate process. This provides the Police Department tighter control over the entry of warrants into their system because the record is not moved until the police department activates it.
2. The warrants can be entered directly into the Wanted System provided from JIS. Management reports are produced and forwarded to the police department responsible for the warrants.

Both options require the Court to extract warrant entry/recall requests using a predefined file layout and send them to REJIS via FTP. Note! Both the 21st and 22nd Judicial Courts have the front-end processing logic to extract the warrant information from JIS. REJIS can assist "DIVISION" in acquiring the necessary logic.

Integrated Jail Management System (IJMS) Interface - REJIS developed a jail management application, known as IJMS, that is used by St. Louis City, St. Louis County and the Jefferson County Sheriff's Office. Information contained in IJMS can be viewed and/or managed from any networked computer in the correctional facility depending on the user's level of access. Information included in IJMS are inmate classification, medical status, property location, commissary accounts, scheduling, visitors, transportation, warrant processing, incidents and grievances, event logging, release processing, among many others. The system also provides paperless event journalizing, staff assignments, and scheduling.

- IJMS utilizes a number of interfaces to make information seamless and more consistent across systems and between agencies.
- LEWeb - Arrest records can be used to populate the inmate's record to reduce keystrokes. In addition, summarized profiles of inmates are available from the LEWeb portal.
- HNS - Information is sent to the REJIS Hit Notification System when an inmate is booked through IJMS. Another notification is sent when the inmate is released.
- MEDIA SERVICES Mug shots - Housing unit cards, line ups, wristbands, and court action notices are produced with a photo of the inmate to aid in inmate control and management.
- LiveScan - Information from IJMS is exported to the LiveScan device to simplify the generation of the fingerprint record.
- MSHP - Fingerprint images are electronically sent to the highway patrol for identification.
- Inmate Phone System - A file of currently incarcerated inmates is transferred via FTP to the vendor every 30 minutes.
- Commissary - Several interactions occur between IJMS and the commissary vendor. These include identifying inmate orders

- with the inmate's ID, proper notification when commissary access is suspended, and tracking an inmate's available funds.
- MOVAN/VINE - Queries can be performed to obtain all inmates released from the facility. Booked and released inmates are also provided in a batch environment to VINE.
- MULES/NCIC - A hot file check is available to query the state and national systems for outstanding warrants.
- Social Security Administration - Incarceration information is provided batch and online.
- 22nd Circuit Court - Incarceration information is sent to the court weekly via FTP.

Security Licensing Interface - The Security Licensing System (SLISYS) is used to administer private security employees by tracking the application and licensing of private security officers, couriers, watchman, and corporate security officers. The application also allows security company administrators the ability to review training and certification status of their employees through the web.

- Hit Notification System - Individuals licensed as security personnel are automatically tracked in the Hit Notification System. When an inquiry is performed on the individual by another agency, the inquiring agency is notified that the person is a licensed security guard and indicates whether he/she may be armed. The licensing entity is also notified that an inquiry was run against the officer.
- Weapon Hot File - When a weapon is being registered to licensed personnel, the weapon can be automatically checked against the MULES and NCIC files to determine if it is stolen, lost, recovered, etc.
- Hot File - The individual's name and pedigree are used to run a hot file inquiry that searches local files for past criminal history. By law, state and federal files, must be done through a fingerprint match.
- LiveScan - Using the Personnel ID assigned to an individual, the necessary pedigree information is pulled from Security Licensing to populate an associated LiveScan record to create the fingerprint record to complete the criminal background check.

S. Reports in LEWeb

There are numerous reports available from the law enforcement portal and from all other applications developed by REJIS. Reports are delivered by an email notification instructing the recipient to access the report on the REJIS Extranet.

Report set up must be requested through the REJIS Help Desk. The reports are generated at the listed frequency and delivered by an email notification

instructing the recipient to access the report on the REJIS Extranet using their REJIS ID.

REJIS will provide required documentation including diagrams, file layouts, and sample code to aid department personal in the design, development, testing, and implementation of management information system type reports. Once a report has been created by "DIVISION" department personal, running of the report is considered part of the departments subscription and there is not a per run charge associated with the execution/running of the report.

Once created, running of the report is considered part of the departments subscription and there is not a per run charge associated with the execution/running of the report. "DIVISION" will also have access to any new reports as they are developed for other customers that utilize REJIS LEWeb services at no additional charge. Generally, all requests for the running of a report can be scheduled and processed during normal business hours. Any processor intensive reporting requests may be deferred and run during evening hours to limit any impact on mission critical services to REJIS customers.

REJIS will retain responsibility for developing and maintaining all integrated operational type reports.

Each report available in this agreement for LEWeb is listed below.

Law Enforcement Reports

TITLE	DESCRIPTION	REPORT	JOB	FRQ
Arrest				
Arrest Without Disposition	Displays arrest records that do not have dispositions on each charge code on the record.	AR0245	LJAR0007	O
24 Hour Monitor	Displays a list of those who have been arrested and approaching the 24 hour limit.		LGAR0200	1/2 hour
Monthly Arrest Statistics	Monthly Arrest Statistics	LGAR0008	LJAR0004	M
Monthly Arrests Statistics	Monthly arrest statistics by agency - Maplewood, Olivette, Richmond Heights, Shrewsbury, Webster Groves	LRAR0008-A	LJAR0004	M
Daily Auto Theft/Tampering Arrests	Local arrests for tampering and auto thefts	LRAR0009-A		
Monthly Incarceration Totals	Monthly Incarceration Totals	LGAR0055	LJAR0005	D
MOBAR Arrest Watch Summary	MOBAR Arrest Watch Summary	LGAR0212	LJAR0050	M
			LJAR0211	D
			LJAR0214	D
			LJAR0260	M
Not Released in 5 Days Report	Displays individuals not released within 5 days that do not have a disposition.	AR0260A		
Incarceration of Females Only	Displays a list of females that have been arrested for an agency during a specified period.	AR050F	LJAR050F	M
Incarceration of Males Only	Displays a list of males that have been arrested for an agency during a specified time frame.	AR050M	LJAR050M	M
Arrests Without Judicial Disposition	Displays arrest records that do not have a judicial disposition on the arrest.	AR0901A	LJAR0901	O
DWITS State Error Report	DWITS State Error Report	LGARDWTE	LJAREWIT	D
Released Pending Application of Warrant	Displays arrest records that were released with a disposition code of RPAW (released pending application of warrant) that are older than 10 days.	RPAW	LJARRPAW	D
YTD Arrests by Officer	St. Peter's Police Dept. year-to-date arrests by officer	LRAR0021-A	LJARSPET	M
Weekend Release Reports	Weekend Release Disposition			
		WRTPOL - City PD's	LJARWRP1	W
Watch Summary	Watch Summary Information	WRPTCRT - City Court's	LJARWRP2	
Prisoners to be Released	Arrest Response to 24 Hour Release	Video report	LTARTINQ	O
Confined Prisoners	Confined Prisoners List	Video report	LTARTINQ	O
		Video report	LTARTINQ	O

TITLE	DESCRIPTION	REPORT	JOB	FREQ
Gang				
Gang Member Enter Report	Gang members entered by/for "DIVISION"	Gang Enter	AJACNGE	W
Gang Member Arrest Report	St. Louis City Circuit Attorney gang member arrest report	AQHSNGR	AHSGNGR	W
Alpha Gang Members List by Nickname	Gang Members Entered During Month	LRGT1002	LJGTQ01B	M
Alphabetic Gang Members Listing	Gang Members Entered During Month	LRGT1001	LJGTQ01B	M
Missing Persons				
St. Louis County Missing	Missing entries and cancellations for St. Louis County	LGWP001A-1	LJWP001A	D
Missing Persons Report	General Missing Persons display report	LGWP500B-1	LJWP500Q	M
NCIC				
Entered Articles and Guns Report	Report listing articles, stolen guns and recovered guns to "DIVISION"	EARPT EGRPT	LJZN001A	D
Charge Codes				
Charge Code Listing	Charge Code Listing (Charge Code order)	ARSW0005	AJSW0005	O
Charge Code Listing	Charge Code Listing (Keyword order)	ARSW0015	AJSW0015	O
Traffic Analysis				
Vehicle Stop Reports	Attorney General Vehicle Stop reporting for each agency.	XX050AA	LJXX050A	A
Vehicle Stop Reports	Monthly Vehicle Stop reporting for each agency.	XX050AA	LJXX050M	M
Vehicle Stop Reports	Vehicle Stop reporting for any agency, specify date range.	XX050AA	LJXX050R	O
Warrants				
Entered/Cancelled Warrants	Listing of all warrants entered or cancelled by St. Louis City and/or St. Louis County on the previous day.	SL6L	LJWP001	D
Out of State Felony Warrants	Print out-of-state warrants (except for traffic) that have been entered in the last 30 days.	LRWP0405	LJWP0405	M
Purged and Pre-Purged Criteria for WNT	Listing of criteria to purge wanted records.	LRWP0101	LJWP101A	M
Police Dept. Purge Report	Reports of Wanted records purged.	LRWP0101	LJWP101A	M
Pending Warrant Purge	Reports of Wanted records about to be purged.	LRWP0101	LJWP101A	M
Warrant Count	Count of warrants for St. Louis County	LRWP299B	LJWP299B	M
Wanted Validation Reports	Agency gets 1/12 of their records to validate all data.	WP300B1	LJWP300A	M
Northwoods Warrant Cancel Report	List all cancelled warrants for Northwoods PD	LGWP000-1	LJWP401F	W

List Suppressed Warrants

TITLE

Suppressed indictments entered yesterday for "DIVISION"	REPORT	JOB	FRQ
DESCRIPTION			
21st Judicial Circuit Court St. Louis County municipal "Division" Daily Warrant Executed Report	LQWPWCN1-A	LJWPWCAN	D
Display wanted record from purge tape by REF or Name	LRWP925A-A	LJWP925A	O
Display wanted record from purge tape by Date Range, ORI, TPC and record type.	LRWP925B-A	LJWP925B	O
Display wanted record from purge tape by Date Range, ORI and vehicle data.	LRWP925C-A	LJWP925C	O
Display wanted record from purge tape by Date Range, ORI and Jurisdiction of felony or misdemeanor.	LRWP925D-A	LJWP925D	O
Display wanted record from purge tape by Date Range, ORI and vehicle color.	LRWP925E-A	LJWP925E	O
Display wanted record from purge tape by Date Range, ORI and zip code (home, work, school and frequented).	LRWP925F-A	LJWP925F	O
Display wanted record from purge tape by DOB Range, ORI and pedigree (race, sex, eyes and hair) WNT and/or MIS.	LRWP925G-A	LJWP925G	O
Display wanted record from purge tape by Date Range, ORI and residential state (not Missouri). WNT and/or MIS	LRWP925H-A	LJWP925H	O
Display wanted record from purge tape by Date Range and ORI. Will return all missing juvenile records.	LRWP925I-A	LJWP925I	O
Display wanted record from purge tape by Date Range, ORI and Search-word from the Remarks field. WNT and/or MIS.	LRWP925J-A	LJWP925J	O
Display wanted record from purge tape by Date Range, ORI and NCIC Major Class (up to 5 NCIC majors).	LRWP925K-A	LJWP925K	O

Search Wanted Purge Tape (ROD)

Wants/Warrants

Daily Warrants Cancelled

	Display wanted record from purge tape by Date Range, ORI, Race, Sex, and DOB.	LRWP926A-A	LJWP926A	O
	Display wanted record from purge tape by Date Range, ORI, and up to 5 charge codes.	LRWP927A-A	LJWP927A	O
	Display wanted record from purge tape by Date Range, ORI, License and VIN.	LRWP928A-A	LJWP928A	O
	Display wanted record from purge tape by Date Range, ORI, Race and Sex, WNT and/or MIS.	LRWP929A-A	LJWP929A	O
Validations				
Guns Record Validation	Agency letter, certification of validation, validation report and audit report for Guns.	ZM300BA Guns Print	LJZM300	M
Securities Record Validation	Agency letter, certification of validation, validation report and audit report for Securities.	ZM300BB Guns Audit		
Boats Record Validation	Agency letter, certification of validation, validation report and audit report for Boats.	ZM300CA Securities Print	LJZM300	M
Protection Order Validation	Agency letter, certification of validation, validation report and audit report for Protection Orders.	ZM300CB Securities Audit		
		ZM300EA Boats Print	LJZM300	M
		ZM300EB Boats Audit		
		ZM300FA Protection Print	LJZM300	M
		ZM300FB Protection Audit		
Sexual Offenders	Agency letter, certification of validation, validation report and audit report for Sexual Offenders.	ZM300GA Sexual Offenders Print	LJZM300	M
		ZM300GB Sexual Offenders Audit		
TITLE	DESCRIPTION	REPORT	JOB	PRO
Vehicles				
Daily Autotheft Report	Daily stolen vehicle report - vehicles entered	LGVH001BA	LJVH001	D
Daily Autotheft Recovery Report	Daily stolen vehicle report - vehicles canceled	LGVH001BA	LJVH001	D
Active Stolen Report	Stolen vehicle report broken down by passenger vehicle, trucks and motorcycles. The passenger vehicles are broken down by Manufacturer.	GMPASS, CHRYP, FORDPS, LJVH001		W
		OTHRPS, TRUCKS,		
		MTRCYC, TRAILR,		
		MISCVH, VINPLT, TRANSM & ENGINE		
Annual Stolen Report	Stolen vehicle report broken down by passenger vehicle, trucks, and motorcycles. The passenger vehicles are broken down by Manufacturer.	GMPASS, CHRYP, FORDPS, LJVH001		A
		OTHRPS, TRUCKS,		
		MTRCYC, TRAILR,		
		MISCVH, VINPLT, TRANSM & ENGINE		

TITLE	DESCRIPTION	REPORT	JOB	FRQ
Vehicles				
Located / Uncancelled Reports	Report of vehicles located at least 3 days and not yet cancelled.	PRNTFL (LGVH101A)	LJVH001	W
Stolen Vehicle Status Reports	STL CO PD quarterly stolen vehicle reports	LGVH300F	LJVH001	Q
List of all Vehicles Stolen in a Year	"DIVISION" annual report of stolen vehicles previous year	LGVH300G	LJVH001	A
Vehicle Asset Report	Asset removal report	LGVH005A	LJVH005A	D
Asset Forfeiture Report	Print "DIVISION" Asset Removal/Forfeitures (VPS email)	ASSETRPT	LJVH005A	D
Active Tow records for "DIVISION"	All Tow records in last 7 days that "DIVISION" sends to DOR (other than abandoned or derelict vehicles)	DORREPT	LJVH103A	W
Print Purge Reports	Listing of purged vehicle records for each agency having purged vehicles.	LGVH203B	LJVH203	M
Vehicle System Statistical Report	REJIS report of all counts of activities of Vehicle System	VH299A Detail VH299B Summary VH400V	LJVH299A	M
Vehicle Validation Reports	Print vehicle validations for "DIVISION" and other agencies.		LJVH400A	M
Vehicle Validation Labels	Print vehicle validation labels for all ORI.	VH401AT LBLs	VH401AA LJVH401A	M
Vehicle Summary Report	Lists stolen, wanted, towed or all vehicle records for one ORI	LGVH500B	LJVH500A	O
Select Data for Summary Program	Lists towed vehicles from previous month for 1 ORI	LGVH501B	LJVHSLCT	O
Search Vehicle Purge Tape (ROD)	Display vehicle record from purge tape by REF, VIN, LIC, TPC or DSN.	LRVH925A-A	LJVH925A	O
Search Vehicle Database (ROD)	Display vehicle record from database by Date Range, OCA, DSN and ORI.	LRVH925B-A	LJVH925B	O
	Display vehicle record from database by Date Range, ORI, LIC and Category.	LRVH925C-A	LJVH925C	O
	Display vehicle record from database by Date Range, ORI and TPC.	LRVH925D-A	LJVH925D	O
	Display vehicle record from database by Date Range, ORI, Category, Vehicle Year, Vehicle Make, and Vehicle Model	LRVH925E-A	LJVH925E	O
	Display vehicle record from database by Date Range, Vehicle Year, Vehicle Make, Vehicle Model and Vehicle Colors.	LRVH925F-A	LJVH925F	O

TITLE Vehicles	DESCRIPTION	REPORT	JOB	FRO
	Display vehicle record from database by Date Range, ORI and parts Category.	LRVH925G-A	LJVH925G	0
	Display vehicle record from database by SHP.	LRVH925H-A	LJVH925H	0
	Display active tow records from database for one ORI.	LRVH925I-A	LJVH925I	0
	Display active Category 36 records from database for one ORI.	LRVH925J-A	LJVH925J	0
	Display vehicle record from database by Date Range, Owner, City, State, Zip and Category.	LRVH925K-A	LJVH925K	0
	Display vehicle record from database by Date Range, ORI and multiple Categories.	LRVH925L-A	LJVH925L	0
	Display vehicle record from database by Date Range, ORI, Category, Vehicle Year, Vehicle Make and Vehicle Model.	LRVH925M-A	LJVH925M	0
	Display vehicle record from database by Date Range, ORI, Category, Vehicle Year, Vehicle Make and Vehicle Model.	LRVH925N-A	LJVH925N	0
	Display tow records from database by Date Range and ORI.	LRVH925O-A	LJVH925O	0

TITLE	DESCRIPTION	REPORT	JOB	FRQ
Vehicles Search Vehicle Database (ROD)	Display vehicle record from purge tape by Date Range, ORI and Category.	LRVH926A-A	LJVH926A	O
	Display vehicle record from purge tape by Date Range, ORI, Category, Vehicle Year, Vehicle Make and Vehicle Model.	LRVH927A-A	LJVH927A	O
	Display vehicle record from purge tape by Date Range, ORI, OCA and DSN.	LRVH928A-A	LJVH928A	O
	Display vehicle record from purge tape by Date Range, ORI and IPC.	LRVH929A-A	LJVH929A	O
	Display vehicle record from purge tape by Date Range, Vehicle Type, Vehicle Make, Vehicle Model, Vehicle Color and Vehicle Year.	LRVH930A-A	LJVH930A	O
	Display vehicle record from purge tape by SHP.	LRVH931A-A	LJVH931A	O
	Display vehicle record from purge tape by Date Range, Owner City, State and Zip.	LRVH932A-A	LJVH932A	O
	Display vehicle record from purge tape by Date Range, ORI, Category, Vehicle Make, Vehicle Style and Vehicle Type.	LRVH933A-A	LJVH933A	O
	Display vehicle record from purge tape by Cancel Date, ORI and Category.	LRVH934A-A	LJVH934A	O

